Administració Oberta de Catalunya

PLEC DE PRESCRIPCIONS TÈCNIQUES PER A LA CONTRACTACIÓ DELS SERVEIS DE CERTIFICACIÓ DIGITAL
AOC-2025-2

Generalitat de Catalunya

LOCALRET

Realitzat per: Servei de Certificació Digital
Versió: 1.5
Data: 24/7/2024
Arxiu: PPT_SCD_2025_v.1.5.docx

INDEX

1 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 i en relació a l'objecte d'aquest contracte, s'ha de considerar al Consorci AOC, a tots els efectes, com a Prestador Qualificat de Serveis de Certificació.

En relació a l'àmbit dels Serveis de Certificació Digital (SCD) i aquells d'altres que en són connexos, vinculats o relacionats, estem davant d'uns serveis d'alta criticitat i complexitat, amb moltes particularitats, una gran quantitat d'usuaris consumint els serveis de manera concurrent, així com una important dependència estratègica amb els serveis digitals dels ens i organismes públics de l'àmbit català usuaris dels serveis.

Per tant, cal evidenciar ja en aquest punt, que la imprescindible continuat del servei obliga a una constant anàlisi i adequació normativa, com també en relació a les auditories internes i externes que aquesta normativa obliga a realitzar al prestador qualificat de serveis de certificació.

En tractar-se el SCD d'un servei sense solució de continuïtat contractual, s'ha d'iniciar un expedient de contractació que garanteixi la continuïtat de la prestació del servei. Així l'objecte d'aquest Plec de prescripcions tècniques particulars és regular les condicions d'execució del mateix.

2 ABAST DEL SERVEI

Tot i considerar-se com un tot la provisió del servei d'identificació digital, s'ha pogut identificar i considerat necessària l'estructuració del servei en tres lots, que tot i tenir identitat pròpia i diferenciada entre ells, no es poden concebre de manera independent en relació a la prestació global del servei de certificació. En concret:

a. Lot 1: Assessorament en compliment de la normativa d'identificació i signatura electrònica i normativa de protecció de dades de caràcter personal, execució d'auditories internes i suport i acompanyament intern al Consorci AOC en el procés d'execució de les auditories externes.
b. Lot 2: Auditories de conformitat de les Entitats de Registre.
c. Lot 3: Serveis de certificació digital.

3 MARC NORMATIU

La base normativa sobre la qual s'ha d'estructurar el servei és, a tall d'exemple, la indicada a continuació, sempre en el benentès que serà d'aplicació la versió vigent de la legislació aplicable i tota aquella normativa que pugui sorgir durant el temps d'execució del contracte. Per tant, el licitador haurà d'adequar la prestació del servei d'acord amb els requeriments legals establerts en tot moment.

- **Llei 6/2020**, d'11 de novembre, reguladora de determinats aspectes dels serveis electrònics de confiança.
- **Llei 34/2002**, d'11 de juliol, de serveis de la societat de la informació i de comerç electrònic.
- **Reglament (UE) nº 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 pel qual es deroga la Directiva 95/46/CE (Reglament general de protecció de dades, RGPD) i la normativa específica vinculada.
- **Llei orgànica 3/2018**, de 5 de desembre, de protecció de dades personals i garantia dels drets digitals (LOPDGDD).
- **Reial Decret 311/2022**, de 3 de maig, pel que es regula l'Esquema Nacional de Seguretat (ENS).
- **Reial Decret 4/2010**, de 8 de gener, pel que es regula l'Esquema Nacional d'Interoperabilitat en l'àmbit de l'Administració Electrònica (ENI).
- **Reglament (UE) nº 910/2014** del Parlament Europeu i del Consell, de 23 de juliol de 2014, relatiu a la identificació electrònica i els serveis de confiança per a les transaccions electròniques en el mercat interior i pel qual es deroga la Directiva 1999/93/CE (ReIDAS).
- **ETSI EN 319 401 V3.1.1 (2024-06)** General Policy Requirements for Trust Service Providers.
- **ETSI EN 319 411-1 V1.4.1 (2023-10)** Policy and security requirements for Trust Service Providers issuing certificates; Part 1: General requirements.
- **ETSI EN 319 411-2 V2.5.1 (2023-10)** Policy and security requirements for Trust Service Providers issuing certificates; Part 2: Requirements for trust service providers issuing EU qualified certificates
- **ETSI EN 319 421 V1.2.1 (2023-05)** Policy and Security Requirements for Trust Service Providers issuing Electronic Time-Stamps.
- **ETSI EN 319 412-1 V1.5.1 (2023-09)** Certificate Profiles; Part 1: Overview and common data structures.
- **ETSI EN 319 412-2 V2.3.1 (2023-09)** Certificate Profiles; Part 2: Certificate profile for certificates issued to natural persons.
- **ETSI EN 319 412-3 V1.3.1 (2023-09)** Certificate Profiles; Part 3: Certificate profile for certificates issued to legal persons.
- **ETSI EN 319 412-4 V1.3.1 (2023-09)** Certificate Profiles; Part 4: Certificate profile for web site certificates.
- **ETSI EN 319 412-5 V2.4.1 (2023-09)** Certificate Profiles; Part 5: QCStatements.
- **CA/Browser Forum V2.0.4 (17 abril 2024)** Baseline Requirements for the Issuance and Management of Publicly-Trusted TLS Server Certificates
- **ETSI EN 319 403-1 V2.3.1 (2020-06)** Trust Service Provider Conformity Assessment; Part 1: Requirements for conformity assessment bodies assessing Trust Service Providers.
- **ETSI TS 119 403-2 V1.3.1 (2023-03)** Trust Service Provider Conformity Assessment; Part 2: Additional requirements for Conformity Assessment Bodies auditing Trust Service Providers that issue Publicly-Trusted Certificates

ETSI TS 119 403-3 V1.1.1 (2019-03) Trust Service Provider Conformity Assessment; Part 3: Additional requirements for conformity assessment bodies assessing EU qualified trust service providers

- **Mozilla Root Store Policy V2.9 (1 setembre 2023)**
- **Política de Seguretat i Marc Normatiu del Consorci AOC** publicat a la web www.aoc.cat

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

4 Lot 1: ASSESSOREMENT EN COMPLIMENT DE LA NORMATIVA D'IDENTIFICACIÓ I SIGNATURA ELECTRÒNICA I NORMATIVA DE PROTECCIÓ DE DADES DE CARÀCTER PERSONAL EXECUCIO D'AUDITORIES INTERNES I SUPORT I ACOMPANYAMENT INTERN AOC EN EL PROCÉS D'EXECUCIÓ DE LES AUDITORIES EXTERNES.

4.1 Descripció

Derivat de les necessitats del Consorci AOC en complir amb els requeriments de la normativa d'identificació i signatura, en especial del ReIDAS, es requereix d'un procés constant de revisió, actualització i control en les actuacions que conformen el Servei de Certificació Digital.

L'objectiu es disposar d'informació actualitzada, normalitzada i adaptada del Servei de Certificació Digital, davant el constat canvi que pateix el marc normatiu.

El servei requereix d'accions focalitzades en tres eixos:

- Assessorament en compliment de la normativa d'identificació i signatura electrònica, de la normativa de protecció de dades de caràcter personal i d'altres consultes jurídiques.
- Execució d'auditories internes en el marc ReIDAS
- Defensa davant entitats de certificació i els organismes que siguin necessaris de les acreditacions ReIDAS

4.1.1 Assessorament en compliment de la normativa d'identificació i signatura electrònica, normativa de protecció de dades de caràcter personal i altres consultes jurídiques

Els canvis en la legislació i el marc normatiu suposa un procés continu d'adaptació i actualització de la documentació necessària per l'execució del Servei de Certificació Digital. Això requereix d'un esforç per donar resposta al compliment de requeriments dels usuaris i de les parts interessades.

El Consorci AOC requereix del suport en el compliment de la normativa d'identificació i signatura electrònica, en especial pel que fa als criteris de seguretat i operacions en entorns de certificació digital, així com en el compliment de la normativa de protecció de dades personals, i el suport en altres consultes jurídiques que el servei pugui necessitar.

En l'àmbit de la protecció de dades, l'assessorament es farà mitjançant informe que es sotmetrà a la consideració del delegat de protecció de dades del Consorci AOC i que caldrà aclarir o esmenar en funció del resultat d'aquesta.

Aquesta tasca es concreta en la redacció i/o revisió de la documentació jurídica del Servei de Certificació Digital. L'empresa adjudicatària haurà de gestionar les revisions, modificacions,

etc., adaptant a la normativa actual o a les necessitats del servei o del consorci AOC de la documentació jurídica auxiliar del servei de certificació digital que inclou:

- Declaracions de pràctiques de certificació
- Polítiques de certificació
- Textos de divulgació
- Perfils dels certificats
- Condicions especifiques del servei

I qualsevol altra que sigui necessària per al correcte desenvolupament del servei objecte d'aquest contracte.

4.1.2 Execució d'auditories internes

De forma anual el Consorci AOC ha de desenvolupar auditories internes sobre el marc ReIDAS per la totalitat del Servei de Certificació Digital. Aquest és un requisit normatiu que emana de la normativa tècnica aplicable que pretén fer una prova d'esforç del servei per tal de garantir els controls de seguretat pertinents. En aquest punt l'adjudicatari també realitzarà tasques de suport i acompanyament en l'anàlisi de les mateixes.

4.1.3 Suport i acompanyament intern al Consorci AOC en el procés d'execució de les auditories externes

De forma bianual el Consorci AOC ha de sotmetre's al control de l'organisme de supervisió estatal, és a dir, per validar els controls de seguretat del Servei de Certificació Digital. D'aquesta manera es procedeix a la renovació de les certificacions necessàries per complir amb el requeriments del Ministeri a efectes de ser considerat com a Prestador de serveis de confiança qualificat.

Anualment, els Prestadors de serveis de certificació tenen la recomanació de realitzar auditories de control de l'execució de les seves tasques.

Cal destacar la importància del resultat d'aquestes auditories i les que en qualsevol moment pugui efectuar l'organisme de supervisió, atès que poden suposar la retirada de la consideració com a prestador qualificat de serveis de confiança. També cal tenir en compte que el resultat de les auditories seran informades a l'autoritat de protecció de dades corresponent per part de l'organisme de supervisió en cas de possibles infraccions de les normes sobre protecció de dades.

El suport i l'acompanyament intern inclou l'anàlisi i esmena dels possibles incompliments advertits en els resultats obtinguts.

4.2 Funcions

4.2.1 Funcions de l'adjudicatari cap al Consorci AOC

L'empresa adjudicatària presentarà al cap de servei, la relació del personal adscrit al servei, especificant les categories de cada un dins de l'estructura, que en tot cas haurà de disposar de la qualificació, coneixements i experiència necessaris per a la prestació del serveis de certificació oferts i els procediments de seguretat i gestió adequats en l'àmbit de la signatura electrònica.

L'empresa adjudicatària aportarà la informació relativa a procediments de treball, treballs efectuats i temps invertits. Igualment informarà de qualsevol defecte o anomalia a les instal·lacions durant el desenvolupament de les seves activitats.

4.2.1.1 Governament de la seguretat

La finalitat del governament de la seguretat es focalitza en vetllar per una correcta gestió de la seguretat de la informació del Consorci AOC al llarg de tot el seu cicle de vida.

Aquest objectiu s'assolirà mitjançant:

- La prescripció, seguiment i verificació de la correcta implantació del model de seguretat
- El compliment dels requeriments que siguin d'aplicació d'acord amb el Marc Normatiu vigent de AOC i de la Generalitat de Catalunya vigent i amb les modificacions que es produeixin al llarg de la prestació del servei, així com del marc legal que en sigui d'aplicació
- En relació al tractament de dades de caràcter personal, l'adjudicatari donarà compliment com a encarregat de tractament a allò establert a la normativa vigent en matèria de protecció de dades de caràcter personal i a l'establert a l'encàrrec de tractament.
- La implantació dels controls de seguretat que permetin mitigar els riscos als que la informació del Consorci AOC i els seus sistemes estan exposats

L'adjudicatari haurà de tenir en compte la classificació de la informació que tracta o genera, objecte del contracte, per aplicar correctament el marc normatiu i legal del Consorci AOC en matèria de seguretat.

En el cas que l'adjudicatari presti serveis o emmagatzemi informació vinculada al servei fora de les instal·lacions del Consorci AOC, haurà de garantir i demostrar l'aplicació de les mesures de prevenció i protecció d'acord als estàndards de la Generalitat de Catalunya en les dependències des de les que presta el servei.

4.2.1.2 Governament de la continuïtat i la disponibilitat

La finalitat del governament de la continuïtat i la disponibilitat se centra, principalment, en garantir la continuïtat del servei i processos davant de qualsevol situació adversa, evitant un impacte significatiu en l'organització.

Els objectius que es persegueixen són:

- Disposar de mecanismes per garantir la continuïtat del personal involucrat en les auditories.
- Disposar d'un pla de continuïtat dels processos, persones i sistemes d'informació que participen en el procés d'assessorament.
- Garantir la continuïtat del servei.
- 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.

4.2.2 Funcions del Consorci AOC cap a l'adjudicatari

El Consorci AOC serà responsable de donar accessos a les xarxes corporatives i col·laborarà en tot moment amb l'adjudicatari en la realització de les tasques descrites. Totes les comunicacions es realitzaran mitjançant l'eina de *tiqueting* que faci servir el Consorci AOC i per tant el Consorci AOC haurà de facilitar els usuaris o llicències que siguin necessaris per al correcte desenvolupament de les tasques.

El Consorci AOC facilitarà tota la informació de la que disposi a l'adjudicatari sobre els temes de seguretat i de protecció de dades, així com la interlocució amb els responsables de seguretat i de protecció de dades respectivament.

El Consorci AOC garantirà la interlocució tant amb el cap de servei de certificació com amb el responsable de l'assessorament jurídic del serveis del Consorci AOC.

4.3 Requisits

4.3.1 Requisits personals

Les tasques a desenvolupar en aquest lot s'han calculat a partir de la incorporació (en diferent percentatge) dels perfils següents:

- Consultor ReIDAS
- Auditor intern

En tots els casos, es calcula sobre unes 1700 hores/any persona (inclou, per tant, té en compte els dies de baixa i absències).

El personal adscrit al servei, en conjunt, ha de disposar dels coneixements suficients, tant a nivell tècnic pràctic com d'idiomes (domini del català (nivell C), castellà i anglès), que assegurin la correcta interpretació de procediments i normes de seguretat, fet que ha de permetre una correcta aplicació d'aquests coneixements.

El personal que l'adjudicatari destini a aquest servei haurà de reunir totes les condicions estipulades per la normativa actualment vigent.

El Consorci AOC pot refusar i/o sol·licitar el canvi d'interlocutor o responsables de projecte. En aquest cas, l'adjudicatari ha de reemplaçar al treballador per un altre suficientment capacitat per dur a terme la tasca encomanada. Els costos derivats d'aquesta incidència aniran a càrrec de l'adjudicatari.

El Consorci AOC es reserva el dret de no acceptar el personal que desenvolupi la seva tasca sense una capacitació suficientment o un comportament incorrecte.

Caldrà presentar una taula de correlació entre els mitjans requerits i els presentats per part de l'adjudicatari.

L'adjudicatari s'ha de fer càrrec de tots els materials i útils per a la correcta execució dels serveis encomanats, degudament identificats com de la seva propietat.

El Consultor EIDAS proposat per l'adjudicatari haurà de disposar d'un número de telèfon que permeti la seva localització en jornada laboral del calendari laboral de Barcelona, per part del personal responsable del Consorci AOC.

L'auditor ha de demostrar ser competent per dur a terme l'auditoria. Això inclou la realització de judicis tècnics exigits, la definició de polítiques i la seva implementació i la imparcialitat.

L'empresa adjudicatària acreditarà documentalment que el personal que s'assigni al servei, hagi realitzat prèviament a l'inici de les tasques, els diferents cursos en relació a la formació especifica per al servei, per la que es determinen els programes de formació de seguretat.

En cas de baixa de qualsevol dels membres de l'equip, l'adjudicatari haurà de substituir-lo en menys de 15 dies laborables d'acord amb els responsables del Consorci AOC. Qualsevol canvi en un dels membres de l'equip a instàncies de l'adjudicatari haurà de ser pactat amb el Consorci AOC, que haurà de validar tant la baixa com el currículum de la nova persona a incorporar. Si el canvi és a instàncies de l'adjudicatari, caldrà acordar el calendari de canvi amb el Consorci AOC per tal de minimitzar l'impacte en els desenvolupaments en curs. Resten fora d'aquest compromisos els períodes de vacances i permisos de tots els membres de l'equip.

El Consorci AOC realitzarà, si s'escau, entrevistes a les persones de l'equip de projecte proposat i, si és necessari, demanarà alternatives a les persones presentades.

El Consorci AOC es reserva el dret a demanar el canvi de qualsevol dels membres de l'equip sense necessitat de justificació amb una antelació de 20 dies naturals a la data de substitució.

El Consorci AOC es reserva el dret a demanar una declaració personal de cada un dels auditors per garantir la seva formació i coneixements.

Per tal de poder conèixer la qualificació professional, el licitador presentarà el currículum professional dels candidats que proposin per aquests perfils. El licitador justificarà documentalment la qualificació professional del personal destinat amb la presentació de la documentació compulsada que es detalla a continuació: targeta d'identitat professional i títols professionals. Al currículum professional de cada perfil que proposi per les funcions definides, hi constarà com a mínim:

- nom i cognoms
- qualificació educativa i categoria professional
- experiència i formació
- avaluació de la competència: coneixements de la tecnologia i marc legal aplicable.
- seguiment de l'acompliment
- data de l'actualització més recent de cada registre

4.4 Condicions

4.4.1 Assessorament en compliment de la normativa d'identificació i signatura electrònica, normativa de protecció de dades de caràcter personal i altres consultes jurídiques

Degut a les necessitats recurrents de modificació de la documentació del Servei de Certificació Digital (SCD) polítiques, s'ha decidit establir un calendari fix d'actualitzacions de la documentació.

- La primera actualització es produirà durant el primer semestre de cada exercici.
- La segona actualització es produirà durant el segon semestre de cada exercici.

Les hores previstes en esforç anual per aquest concepte i perfils implicats es mostren en el Plec de Clàusules Administratives. Es calculen unes 1.700 hores/any persona (inclou, per tant, els dies de baixa i absències).

Tasques a executar:

1. Actualització segons recomanacions ETSI
   Coneixement actualitzat de la normativa d'identificació i signatura electrònica, en especial del ReIDAS Gestió del canvi (anàlisi de la capacitat)
   Detecció de necessitats
   Pla d'accions que suposen les necessitats

2. Actualització documentació reguladora del servei de certificació digital
   Gestió del canvi (anàlisi de la capacitat)
   Detecció de necessitats de les DPC i Polítiques
   Pla d'accions que suposen les necessitats
   Redacció dels apartats de compliment normatiu de la documentació
   Assessorament de la resta d'apartats

3. Actualització segons normativa: autonòmica, estatal, europea i internacional
   Gestió del canvi (anàlisi de la capacitat)
   Actualització trimestral dels acords anuals DATASHIELD
   Pla d'accions que suposen els acords
   Resolució d'incidents derivats

4. DATASHIELD (acords internacionals)
   Actualització trimestral dels acords anuals DATASHIELD
   Pla d'accions que suposen els acords
   Resolució d'incidents derivats

5. Execució d'Auditories internes
   Disposar d'Auditors acreditats
   Complir l'abast de l'auditoria
   Generar un programa, pla i un informe

6. Suport en la superació d'auditories:
   Coneixements del sector
   Coneixement de les normes de l'abast
   Atenció a consultes en 48 hores demora màxima

4.4.1.1 Planificació de l'assessorament, revisió i propostes de millora

Les fases del calendari d'actualització ordinària de la documentació seran les següents:

Primer semestre:

- **Gener i febrer,** fase de recollida de propostes de modificació.
- **Març,**
  1. la **primera quinzena** es dedicarà a la fase de anàlisi, comprovació i proposta de calendari
  2. la **segona quinzena** es dedicarà a la comprovació i redacció de les modificacions.
- **Abril,**
  1. la **primera quinzena** es traslladarà la proposta modificada a l'equip del servei del Consorci AOC.

2. la **segona quinzena** es realitzarà una reunió amb l'Àrea proposant, anàlisi dels canvis i aprovació del document.

- **Maig**,
  - 1- a **la primera quinzena** és realització d'una segona reunió, si escau, i preparació dels documents modificats definitius en català, castellà i Anglès
  - 2- la segona quinzena es traslladaran els canvis acordats a l'adjudicatari del lot 3 d'aquesta licitació.

- **Juny**, fase de publicació en la web del Consorci AOC i enviament a tots els organismes que sigui necessari.

Quant al segon semestre:

- **Juliol i agost,** fase de recollida de propostes de modificació.
- **Setembre,**
  - 1. la **primera quinzena** es dedicarà a la fase de anàlisi, comprovació i proposta de calendari
  - 2. la **segona quinzena** es dedicarà a la comprovació i redacció de les modificacions.
- **Octubre,**
  - 1. la **primera quinzena** es traslladarà la proposta modificada a l'equip del servei del Consorci AOC.
  - 2. la **segona quinzena** es realitzarà una reunió amb l'Àrea proposant, anàlisi dels canvis i aprovació del document.
- **Novembre,**
  - 1. a **la primera quinzena** és realització d'una segona reunió, si escau, i preparació dels documents modificats definitius en català, castellà i Anglès
  - 2. la segona quinzena es traslladaran els canvis acordats a l'adjudicatari del lot 3 d'aquesta licitació.

- **Desembre,** fase de publicació en la web del Consorci AOC i enviament a tots els organismes que siguin necessaris.

Malgrat aquestes dues revisions anuals planificades, es pot donar el cas que calgui dur a terme altres modificacions, per motius d'urgència o de necessitat del servei, també s'hauran de realitzar en un període màxim d'un mes des de la data de la detecció de la necessitat.

4.4.1.2 Fase de recollida de propostes de modificació

Les propostes de modificació o actualització de la documentació es poden presentar pel cap de servei corresponents, o bé d'ofici pel propi adjudicatari o a recomanació dels adjudicataris dels altres lots que conformen el present contracte.

Totes les propostes es realitzaran mitjançant un tiquet a l'eina corporativa del Consorci AOC

Totes les propostes rebudes seran arxivades en una carpeta creada a tal efecte, indicant la data de recepció de la proposta, la descripció de la modificació proposada i la seva justificació. Aquesta carpeta serà la carpeta de documentació reguladora dins del directori corporatiu. Aquesta ubicació, durant el període de vigència del contracte pot patir modificacions.

4.4.1.3 Fase d'anàlisi, comprovació i redacció de modificacions

Totes les modificacions proposades han de ser analitzades, en el seu cas realitzant les comprovacions tècniques necessàries i, en cas de resultar necessària la modificació proposada, redactat el seu text.

Les comprovacions podran incloure consultes a altres adjudicataris dels altres lots del contracte o altres àrees del Consorci AOC o a altres departaments o organismes, als efectes necessaris per produir un text correcte i actualitzat.

L'anàlisi de les modificacions proposades s'ha de registrar en un document de control de revisions de cada document afectat, que ha de tenir els següents continguts mínims:

- Una secció amb l'històric de versions del document, que ha d'indicar la versió vigent (publicada) del document, i la versió en revisió.
- Una secció amb les modificacions proposades, per a cada versió del document, per l'oficina de polítiques, que ha d'indicar la data de la modificació, la secció afectada i la descripció o justificació del canvi proposat.
- Una secció amb la disposició de les modificacions proposades, per a cada versió del document, pel servei afectat, que ha d'indicar la data de la modificació, la secció afectada i la descripció o justificació del canvi proposat.

4.4.1.4 Fase de comentari i aprovació

El/s document/s, amb les seves modificacions proposades, ha/n de ser lliurat/s al cap de servei corresponent i a la resta d'àrees a les que s'hagin sol·licitat comprovacions i altres informacions tècniques, per al seu comentari, en les dates acordades al calendari establert.

Es podran realitzar modificacions addicionals en funció dels comentaris rebuts, sens perjudici dels períodes establerts per les següents fases del procediment, i segons s'estableixi en el calendari programat i s'editarà una versió final del/s document/s, que serà/an aprovada pel cap del servei corresponent.

4.4.1.5 Fase de publicació

El/s document/s aprovat/s ha/n de ser publicat/s a la pàgina web del Consorci AOC a l'apartat de regulació corresponent (actualment a https://epscd.aoc.cat/regulacio).

El Cap del servei, mitjançant l'eina de tiqueting interna del Consorci AOC enviarà a la persona responsable de la pàgina web els documents en versió catalana, castellana i anglesa per tal que els publiqui a l'apartat corresponent. Aquesta fase pot variar tant en la ubicació de la publicació com en les persones responsables de l'execució de la mateixa.

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

4.4.2 Execució d'Auditories internes

Anualment, s'haurà de programar, planificar i executar com a mínim una Auditoria interna per tal de verificar el compliment de la normativa d'identificació i signatura electrònica, en especial el ReIDAS, a la totalitat del Servei de Certificació Digital.

Les hores previstes en esforç anual per aquest concepte i perfils implicats es mostren en el Plec de Clàusules Administratives. Es calculen unes 1.700 hores/any persona (inclou, per tant, els dies de baixa i absències).

Després d'acordar la data d'auditoria, s'haurà de fer arribar un pla d'auditoria a tots els implicats on hi consti:

- Objectiu i abast
- Criteris d'auditoria
- Equip auditor
- Documents de referència
- Agenda amb temps d'inici o durada
- Temes de confidencialitat
- Riscos de l'auditoria
- Instruccions de resolució i seguiment

L'Auditoria interna ha de complir criteris de objectivitat i ha de ser realitzada per un auditor acreditat.

D'altra banda, l'auditor ha de ser imparcial i ha de ser percebut com a tal, amb la finalitat de donar confiança a les seves activitats i resultats.

Per tant, s'evitarà:

- Interessos propis
- Autorevisió d'una activitat duta a terme per la mateixa persona
- Defensa o oposició
- Excés de familiaritat
- Intimidació
- Competència

La planificació de l'auditoria s'haurà de dur a terme amb una antelació mínima d'un mes per poder gestionar la disponibilitat dels implicats.

L'auditoria es realitzarà conforme els procediments d'auditoria establerts en el Consorci AOC.

L'adjudicatari haurà de realitzar un informe d'auditoria on hi constin:

- Les troballes
- Àrees de millora
- Observacions
- Les no conformitats

Les no conformitats hauran d'estar referenciades al punt de requisit de norma que incompleixen i que cal resoldre.

Finalment, l'adjudicatari haurà de proposar al Consorci AOC mesures correctores per poder resoldre els incompliments de norma trobats.

4.4.3 Defensa davant Auditories externes

El Consorci AOC, com a Prestador de Serveis de Confiança executa una auditoria biennal (o quan sigui establert) per part d'una entitat acreditada externa per a obtenir un nivell d'acompliment adequat respecte als requisits especificats en el Reglament (UE) Nº 910/2014 del parlament europeu i del consell de 23 de juliol de 2014, relatiu a la identificació electrònica i els serveis de confiança per a les transaccions electròniques en el mercat interior i per la que es deroga la Directiva 1999/93/CE, i les seves guies de referència (Reglament ReiDAS).

L'abast de la certificació comprèn allò que dictamini l'organisme de supervisió nacional estatal en cada moment.

El Consorci AOC, a través de l'entitat certificadora, informarà amb antelació a l'adjudicatari sobre la planificació de les auditories externes.

L'adjudicatari haurà de fer la defensa davant d'auditories externes que realitzi el Consorci AOC. Per tal de realitzar correctament aquesta defensa, caldrà tenir un ampli coneixement del marc legal que aplica, els requisits legals i requeriments interns del Consorci AOC, així com del resultat de les auditories internes realitzades prèviament.

La defensa inclou l'assistència a l'auditoria, la participació en la presentació d'evidències i la proposta d'accions correctives per tal de solucionar les No conformitats trobades.

Les hores previstes en esforç anual per aquest concepte i perfils implicats es mostren en el Plec de Clàusules Administratives. Es calculen unes 1.700 hores/any persona (inclou, per tant, els dies de baixa i absències).

4.5 Acords de nivell de servei (ANS)

El funcionament del servei objecte d'aquesta contractació estarà subjecte a un sistema de control de qualitat exercit pel Consorci AOC.

El funcionament d'aquest control de qualitat està lligat a les Condicions Generals dels Serveis del Consorci AOC, les Condicions Particulars dels Serveis de Certificació Digital i el marc normatiu aplicable. Els criteris de valoració i puntuació de la qualitat del servei s'esmenten a continuació en cada ANS aplicable.

Aquesta puntuació és important, ja que a part de ser una mesura de qualitat de funcionament del servei, també pot constituir una causa justificada de rescissió del contracte per part del Consorci AOC.

Els acords de nivell de servei (ANS) pel seguiment del servei objecte d'aquest lot seran:

a. Actualització segons recomanacions ETSI
   Número d'incidents per manca de coneixement per sota del 5%.

b. Actualització de la normativa reguladora del servei de certificació digital (Declaració de pràctiques de certificació, polítiques de certificació, etc.)
   Número de revisions detectades, temps entre detecció i modificació

c. Lliurament d'informes de servei lliurat els primers 5 dies operatius del mes següent al que s'està validant
   Es considerarà desviació si l'informe es lliura a partir del 5è dia operatiu del mes.

d. Actualització segons normativa: autonòmica, estatal, europea i internacional.
   Número d'incidents per manca de coneixement per sota del 5%

e. DATASHIELD (acords internacionals)
   Número d'incidents per manca de coneixement en el cas d'Auditories internes per sota del 5%.
   Termini d'execució d'acord al previst en normativa i valor afegit de les propostes de millora.

f. Suport en la superació d'auditories:

Número de no conformitats d'auditoria per sota del 5%.

g. Consultes sobre el marc normatiu del Servei de Certificació Digital: termini màxim d'avaluació i primera resposta 5 dies laborables. En el cas de consultes sobre certificats urgents es redueix a 2 dies

4.6 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'eficaç implantació dels controls definits.

4.6.1 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 determinin en els diferents àmbits del governament del servei objecte d'aquest lot. 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 format i el contingut mínim de la informació a elaborar per l'adjudicatari en tots els àmbits de governament és el definit en l'Annex "Annex _1_Plantilla Informe Seguiment".

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.

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

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

4.6.1.1 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/clients 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

4.6.2 Òrgans de Gestió

4.6.2.1 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 poder adjudicador 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.

4.6.2.2 Reunions de Seguiment.

El gestor del servei de l'adjudicatari i el Cap del Servei del SCD 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 incloses 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.
- 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 proposat en definit en l'"Annex _1_Plantilla Informe Seguiment" que inclou, 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 lot. Nombre de consultes realitzades (per tipologia, telèfon, correu, etc,.).
- Millores aplicables al servei de certificació digital.
- 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.

4.7 Devolució del servei

Un cop finalitzat el contracte l'adjudicatari haurà de garantir que ha complert amb tots els compromisos establerts en aquest lot.

- Informe de situació de compliment normatiu del Consorci AOC. En aquest informe es detallarà quins assessoraments en compliment normatiu d'identificació i signatura electrònica i de protecció de dades personals s'han fet en l'últim any del servei i quin és l'estat actual.
- En el cas que hi hagi, la planificació d'accions previstes envers a compliment normatiu en matèria d'identificació i signatura electrònica i de protecció de dades personals.

- Informes d'auditories internes realitzats durant els últims tres anys al Consorci AOC.
- Estat i seguiment de les propostes d'accions de les auditories internes i de les auditories ReIDAS.
- Anàlisi de riscos i oportunitats detectats en el moment de la finalització del servei d'assessorament i propostes d'actuacions.

L'adjudicatari haurà de retornar tota la informació confidencial propietat del Consorci AOC, així com la generada a partir de la prestació del servei.

L'adjudicatari haurà de finalitzar totes les tasques que li hagin estat encomanades i acceptades abans de la finalització del contracte.

5 Lot 2: AUDITORIES DE CONFORMITAT

5.1 Descripció

L'objectiu de realitzar auditories a les Entitats de Registre que conformen el Servei de Certificació Digital del Consorci AOC (SCD).

Aquest servei engloba 3 subserveis:

- Entitats de registre T-CAT: és un ens o departament que col·labora amb el Consorci AOC en la l'emissió de certificats digitals a les administracions públiques catalanes.
- Entitats de Registres idCAT : és un ens o departament que col·labora amb el Consorci AOC, en el registre de les identitats digitals per a la ciutadania, concretament per a emetre i gestionar certificats idCAT i l'idCAT al mòbil actualment.
- Entitats de registre o Ens subscriptors: és un ens o departament que col·labora amb el Consorci AOC en els tràmits d'identificació, registre i autenticació per a l'emissió de certificats digitals, seguint els procediments i les relacions amb els titulars dels certificats.

Totes aquestes entitats de registre han de complir amb els requeriments i procediments d'emissió i gestió dels certificats idCAT i T-CAT que es realitzen i que compleixen amb els procediments que el Consorci AOC proporciona a les Entitats de Registre (ER's), així com les condicions especifiques del servei i la normativa pròpia del servei de certificació digital com tota aquella que li afecti o pugui afectar, directament.

5.2 Funcions

L'adjudicatari s'haurà de fer càrrec de la realització de les auditories a les ER's (ens subscriptors i entitats de registre T-CAT i idCAT.

L'adjudicatari haurà de dur a terme auditories presencials i virtuals a les ER's, seguint el procediment que el Consorci AOC estableixi, de manera acordada amb l'adjudicatari. El procediment actual es descriu a l'annex 4**.**

A principis de cada any el Consorci AOC acordarà amb l'adjudicatari la selecció de les ER's que s'hauran d'auditar durant aquell any, en base als criteris descrits al citat document; i amb l'objectiu que totes les ER's se sotmetin, com a mínim, a una auditoria presencial cada 2 anys, sempre que hi hagi hagut emissions de certificats. També s'acordarà la planificació de les corresponents auditories.

A mode de resum l'adjudicatari haurà de :

- Realitzar la planificació inicial de la realització de les auditories
- La preparació i organització prèvia de cada auditoria: amb el suport del Consorci AOC i d'acord amb el responsable del servei de cada entitat de registre
- El desplaçament a l'entitat de registre (quan sigui necessari) per a realitzar l'auditoria
- La redacció de l'informe d'auditoria i lliurament al Consorci AOC per a la seva validació
- Un informe final de conclusions (classificat per tipus d'ER) un cop l'any.

L'empresa adjudicatària presentarà al cap de servei, la relació del personal adscrit al servei, especificant les categories de cada un dins de l'estructura.

L'empresa adjudicatària assignarà una persona amb perfil de cap d'auditoria, les principals responsabilitats 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.

L'empresa adjudicatària aportarà la informació relativa a procediments de treball, treballs efectuats i temps invertits. Igualment informarà de qualsevol defecte o anomalia a les instal·lacions durant el desenvolupament de les seves activitats.

5.2.1.1 Governament de la seguretat

La finalitat del governament de la seguretat es focalitza en vetllar per una correcta gestió de la seguretat de la informació del Consorci AOC al llarg de tot el seu cicle de vida.

Aquest objectiu s'assolirà mitjançant:

- La prescripció, seguiment i verificació de la correcta implantació del model de seguretat
- El compliment dels requeriments que siguin d'aplicació d'acord amb el Marc Normatiu vigent de AOC i de la Generalitat de Catalunya vigent i amb les modificacions que es produeixin al llarg de la prestació del servei, així com del marc legal que en sigui d'aplicació
- En relació al tractament de dades de caràcter personal, l'adjudicatari donarà compliment com a encarregat de tractament a allò establert a la normativa vigent en matèria de protecció de dades de caràcter personal i a l'establert a l'encàrrec de tractament.
- La implantació dels controls de seguretat que permetin mitigar els riscos als que la informació del Consorci AOC i els seus sistemes estan exposats

L'adjudicatari haurà de tenir en compte la classificació de la informació que tracta o genera, objecte del contracte, per aplicar correctament el marc normatiu i legal del Consorci AOC en matèria de seguretat.

En el cas que l'adjudicatari presti serveis o emmagatzemi informació vinculada al servei fora de les instal·lacions del Consorci AOC, haurà de garantir i demostrar l'aplicació de les mesures de prevenció i protecció d'acord als estàndards de la Generalitat de Catalunya en les dependències des de les que presta el servei.

5.2.1.2 Governament de la continuïtat i la disponibilitat

La finalitat del governament de la continuïtat i la disponibilitat se centra, principalment, en garantir la continuïtat del servei i processos davant de qualsevol situació adversa, evitant un impacte significatiu en l'organització.

Els objectius que es persegueixen són:

- Disposar de mecanismes per garantir la continuïtat del personal involucrat en les auditories.
- Disposar d'un pla de continuïtat dels processos, persones i sistemes d'informació que participen en el procés d'auditoria.
- Garantir la continuïtat del servei.
- 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.

5.2.2 Funcions del Consorci AOC cap a l'adjudicatari

El Consorci AOC serà responsable de donar accessos a les xarxes corporatives i col·laborarà en tot moment amb l'adjudicatari en la realització de les tasques descrites. Totes les comunicacions es realitzaran mitjançant l'eina de *tiqueting* que faci servir el Consorci AOC i per tant el Consorci AOC haurà de facilitar els usuaris o llicències que siguin necessaris per al correcte desenvolupament de les tasques.

El Consorci AOC facilitarà tota la informació de la que disposi a l'adjudicatari sobre els temes de seguretat i de protecció de dades, així com la interlocució amb els responsables de seguretat i de protecció de dades respectivament.

El Consorci AOC garantirà la interlocució tant amb el cap de servei de certificació com amb el responsable de l'assessorament jurídic del serveis del Consorci AOC.

5.3 Requisits

5.3.1 Requisits generals

L'adjudicatari s'haurà de fer càrrec de:

- Elaborar un pla operatiu d'execució de les auditories de conformitat, ja siguin virtuals o presencials i tenint en compte les economies d'escala en els desplaçaments. És a dir, realitzar totes les auditories d'una mateix organització aprofitant el desplaçament o bé la interlocució, així com aprofitant la proximitat per a realitzar més d'una auditoria a la mateixa jornada.
- Elaborar un pla d'auditoria i comunicar-ho a l'entitat a auditar 30 dies abans de l'execució de la mateixa.
- Executar les auditories de conformitat.
- Disposar d'auditors acreditats
- Elaborar un informe d'auditoria
- Remetre el *Checklist* de seguiment i l'informe d'auditoria al Consorci AOC en un termini màxim indicat al punt "5.5 a Termini de lliurament del checklist i evidències d'auditoria", després de l'execució de l'auditoria, al responsable del servei de certificació digital
- Lliurar un informe d'auditoria a cada ER auditada en el termini màxim indicat al punt "5.5 1-bb Termini de lliurament d'informes", després de l'execució de l'auditoria.
- Avaluar la conformitat de les accions executades per garantir la correcció de les desviacions.

- Realitzar un informe amb un resum de la visió global del grau de compliment dels procediments de les ER, un cop l'any.

5.3.2 Requisits personals

Les tasques a desenvolupar en aquest lot s'han calculat a partir de la incorporació (en diferent percentatge) dels perfils següents:

- Cap d'auditoria
- Auditor acreditat

Per poder oferir tots els serveis objecte d'aquest lot en un escenari de consum màxim, s'han previst, per cada perfil, les hores de dedicació indicades al plec de clàusules administratives.

En ambdós casos, es calcula sobre unes 1.700 hores/any persona (inclou, per tant, es tenen en compte els dies de baixa i absències).

El personal adscrit al servei, en conjunt, ha de disposar dels coneixements suficients acreditats, tant a nivell tècnic pràctic com d'idiomes (domini del català (nivell C), castellà i l'anglès), que assegurin la correcta interpretació de procediments i normes de seguretat, fet que ha de permetre una correcta aplicació d'aquests coneixements.

El personal que l'adjudicatari destini a aquest servei haurà de reunir totes les condicions estipulades per la normativa actualment vigent.

El Consorci AOC pot refusar i/o sol·licitar el canvi d'interlocutor o responsables de projecte. En aquest cas, l'adjudicatari ha de reemplaçar al treballador per un altre suficientment capacitat per dur a terme la tasca encomanada. Els costos derivats d'aquesta incidència aniran a càrrec de l'adjudicatari.

El Consorci AOC es reserva el dret de no acceptar el personal que desenvolupi la seva tasca sense una capacitació suficientment o un comportament incorrecte.

L'adjudicatari s'ha de fer càrrec de tots els materials i útils per a la correcta execució dels serveis encomanats, degudament identificats com de la seva propietat.

El Cap d'auditoria proposat per l'adjudicatari haurà de disposar d'un número de telèfon que permeti la seva localització en jornada laboral del calendari laboral de Barcelona, per part del personal responsable del Consorci AOC.

Per tal de poder conèixer la qualificació professional, el licitador presentarà el currículum professional dels candidats que proposin per aquests perfils. El licitador justificarà documentalment la qualificació professional del personal destinat amb la presentació de la documentació compulsada que es detalla a continuació: targeta d'identitat professional i títols professionals. Al currículum professional de cada perfil que proposi per les funcions definides, hi constarà com a mínim:

- nom i cognoms
- qualificació educativa i categoria professional
- experiència i formació
- avaluació de la competència: coneixements de la tecnologia i marc legal aplicable.
- seguiment de l'acompliment
- data de l'actualització més recent de cada registre

En cas de baixa de qualsevol dels membres de l'equip, l'adjudicatari haurà de substituir-lo en menys de 15 dies laborables d'acord amb els responsables del Consorci AOC. Qualsevol canvi en un dels membres de l'equip a instàncies de l'adjudicatari haurà de ser pactat amb el Consorci AOC, que haurà de validar tant la baixa com el currículum de la nova persona a incorporar. Si el canvi és a instàncies de l'adjudicatari, caldrà acordar el calendari de canvi amb el Consorci AOC per tal de minimitzar l'impacte en els desenvolupaments en curs. Resten fora d'aquest compromisos els períodes de vacances i permisos de tots els membres de l'equip.

El Consorci AOC realitzarà, si s'escau, entrevistes a les persones de l'equip de projecte proposat i, si és necessari, demanarà alternatives a les persones presentades.

El Consorci AOC es reserva el dret a demanar el canvi de qualsevol dels membres de l'equip sense necessitat de justificació amb una antelació de 20 dies naturals a la data de substitució.

El Consorci AOC es reserva el dret a demanar una declaració personal de cada un dels auditors per garantir la seva formació i coneixements.

L'auditor ha de demostrar ser competent per dur a terme l'auditoria. Això inclou la realització de judicis tècnics exigits, la definició de polítiques i la seva implementació i la imparcialitat.

5.4 Condicions

Les entitats de registre es troben distribuïdes per tota la geografia catalana en ajuntaments, consells comarcals, diputacions, universitats, etc...

El número màxim d'auditories d'entitats de registre a realitzar en el marc del present contracte, en modalitat presencial o virtual, serà el definit en les unitats per tipologies definides l'apartat B3 del Plec de clàusules Administratives. A continuació s'exposen les volumetries i condicions aplicables a les tipologies d'auditoria definides :

- Auditories presencials ER T-CAT : actualment hi ha 72 ER T-CAT operatives.
- Auditories presencials ER idCAT: existeixen 282 entitats de registre idCAT de les quals un 70% s'auditarà virtualment i un 30% presencialment, segons les volumetries d'emissions
- Auditories virtuals Entitat de Registre (ens subscriptors): aquestes auditories sempre seran virtuals a excepció de necessitat de presencia per problemes en la primera auditoria virtual: 2.200 organismes
- Auditories virtuals Entitats de Registre idCAT: existeixen 282 entitats de registre idCAT de les quals un 70% s'auditarà virtualment i un 30% presencialment, segons les volumetries d'emissions.

Cada 2 anys el Consorci AOC, com a prestador de serveis de certificació, ha de garantir que les entitats de registre amb emissions han d'haver passat una auditoria. Aquest carència es pot veure afectada per canvis en el marc normatiu o segons els processos de millora continua als que està obligat el servei.

Els esforços en hores previstos per cada perfil i cada tipus d'auditoria s'exposen en el plec de clàusules administratives.

5.4.1 Programa d'auditories

Anualment l'adjudicatari, procedirà a una programació d'entitats a auditar.

Quan un organisme sigui entitat de registre T-CAT i idCAT s'aprofitarà per realitzar les auditories en un mateix desplaçament, en el cas que es determini la necessitat d'una auditoria presencial.

En el cas de les auditories virtuals, també s'aprofitarà el contacte amb l'organització per realitzar les auditories de control que sigui necessàries.

L'equip d'auditoria haurà d'estar en permanent contacte amb les persones que formen el Servei de Certificació Digital i amb l'adjudicatari dels altres lots del present contracte.

El programa de treball i el calendari proposat serà elaborat per el proveïdor. Tot i això, el Consorci AOC podrà decidir quines auditories són prioritàries.

L'adjudicatari haurà d'haver realitzat la totalitat de les auditories planificades en els períodes bianuals que marca el reglament eIDAS.

El proveïdor generarà un pla operatiu del projecte que haurà de contenir tota la informació necessària per a assegurar la qualitat de les auditories realitzades.

5.4.2 Planificació i preparació de l'auditoria

L'objectiu d'aquest pas és obtenir la màxima informació possible de l'entitat de registre abans d'abordar amb èxit l'auditoria. Això inclou:

- Obtenir la fitxa de subscriptor i d'entitat de registre on figuren tots els participants del servei a l'ens amb el seu rol i tota la documentació que sigui necessària.
- Conèixer el nombre de certificats emesos
- Disposar de la data de la darrera auditoria i resultats (en el cas que n'hi hagi)
- Conèixer qualsevol canvi que hagi pogut afectar al servei.
- Disposar del llistat d'incidències sofertes
- Disposar de l'informe de revisió de gestió.

Un cop tancada la data d'auditoria amb l'entitat de registre, caldrà enviar un correu-e amb la planificació detallada de la mateixa al responsable de servei.

El pla d'auditoria haurà d'incloure els següents punts:

- Objectiu i abast
- Criteris d'auditoria
- Equip auditor
- Documents de referència
- Agenda amb temps d'inici o durada
- Temes de confidencialitat
- Riscos de l'auditoria
- Instruccions de resolució i seguiment

La comunicació del pla d'auditoria a l'entitat de registre caldrà fer-la amb 30 dies d'antelació a la realització de la mateixa.

Tota aquesta primera part es pot fer mitjançant telèfon i correu-e amb l'entitat de registre amb un correu electrònic corporatiu que subministrarà el Consorci AOC, però sempre haurà de quedar una constància per escrit.

L'estat de cada actuació ha d'estar sempre disponible per al Consorci AOC mitjançant les eines pròpies del Consorci AOC

5.4.3 Realització pròpiament de l'auditoria

La realització de l'auditoria es realitzarà conforme els procediments d'auditoria establerts i que trobareu en l'annex 4.

5.4.3.1 Les pautes a seguir a l'auditoria presencial serà la següent:

Termes i condicions: Posar a disposició dels subscriptors, les entitats de registre i parts interessades els termes i condicions de cadascun dels serveis prestats. Aquests termes i condicions especificaran:

- Les obligacions del subscriptor i les entitats de registre, si hi ha,
- El període de temps que es guarden els *logs* del servei de confiança
- Les limitacions de responsabilitat
- Marc legal aplicable
- Procediment de queixes i resolució de conflictes
- Informació de contacte del servei de confiança
- Compromís sobre la disponibilitat

Cal informar als subscriptors, les entitats de registre i a les parts interessades dels termes i condicions abans d'iniciar la relació contractual. A més, aquests termes i condicions han d'estar disponibles a través de mitjans de comunicació no peribles, amb un llenguatge entenedor i que es puguin transmetre electrònicament.

Operació i gestió del servei

- Els serveis han de ser accessibles a tots els sol·licitants, les activitats dels quals estan dins del seu camp d'operació declarat i que accepten complir les seves obligacions especificades als termes i condicions del servei.
- Disposar de polítiques i procediments per a la resolució de conflictes o reclamacions de clients o altres parts interessades
- Contracte en vigor amb el Consorci AOC.

Recursos humans involucrats: L'ens s'ha d'assegurar que el personal que dona el servei és responsable i dona confiança al servei donat.

- El personal estarà qualificat per fer la feina encomanada i haurà rebut formació sobre seguretat i protecció de dades personals adequades al servei ofert i el lloc de treball.
- Es disposarà d'una fitxa de personal actualitzada amb la formació rebuda (coneixement, experiència i qualificacions) o experiència en el lloc de treball que s'anirà actualitzant cada any, en funció d'actualitzacions sobre noves amenaces o noves pràctiques de seguretat.
- Es descriuran sancions disciplinàries per aquells treballadors que incompleixin les polítiques o procediments establerts.
- Les funcions de seguretat i les responsabilitats estaran descrites clarament en la descripció dels llocs de treball que estaran disponibles per a tot el personal implicat. Les funcions de confiança, de les que depèn la seguretat de la operació del servei, han d'estar clarament identificades. Les funcions de confiança seran nomenades per la direcció i seran acceptades per la direcció i per la persona implicada.

- Tot el personal (temporal o fixe) disposarà de la seva descripció del lloc de treball on hi constarà la sensibilitat de posició en funció del drets i nivell d'accés, formació i sensibilització.
- Es disposarà de procediments i processos de gestió alineats amb els de seguretat de la informació.
- Tot el personal amb funcions de confiança han d'estar lliures de conflictes d'interessos que puguin perjudicar la imparcialitat de les operacions del servei.
- Les funcions de confiança inclouen:
    - Operador del sistema: Responsable per operar el sistema de confiança en el dia a dia. Autoritzat per realitzar la còpia de seguretat.
- El personal no tindrà accés a les funcions de confiança fins que no s'hagin complert tots els controls necessaris.

Gestió d'actius: L'ens s'haurà d'assegurar del nivell apropiat de protecció dels actius, incloent els actius d'informació.

- Mantenir un llistat actualitzat d'actius d'informació amb l'assignació de la classificació corresponent amb l'avaluació de riscos realitzada.
- Tots els materials es tractaran de manera segura segons la seva classificació de risc. Els materials que continguin dades sensibles es destruiran de manera segura quan ja no siguin necessaris.

Control d'accés digital: L'accés al sistema estarà limitat al personal autoritzat.

- L'accés a la informació i a les funcions del sistema d'aplicació han d'estar restringits d'acord amb la política d'accés.
- El personal de l'ens s'ha d'identificar i autenticar abans d'utilitzar aplicacions crítiques relacionades amb el servei.
- El personal de l'ens es responsable de les seves activitats.
- Ha d'existir un protocol o política d'esborrat segur de dades confidencials en dispositius per tal d'evitar l'accés no autoritzat.

Control d'accés físic: S'ha de controlar l'accés físic als components del sistema de l'ens, la seguretat dels quals és crítica per a la provisió del servei de confiança i minimitzar els riscos relacionats amb la seguretat física.

- Accés físic limitat als components del sistema de l'ens que són crítics per a la prestació del servei.
- S'han d'implementar controls per evitar la pèrdua, dany o compromís d'actius i interrupció de les activitats
- S'han d'implementar controls per evitar el compromís o robatori d'informació i de les instal·lacions de processats de la informació.
- Els components que són crítics per a la prestació del servei han d'estar localitzats en un perímetre de seguretat protegit físicament contra la intrusió i s'ha de controlar l'accés a través d'un perímetre de seguretat i alarma.

Seguretat operacional: L'ens ha d'utilitzar sistemes de confiança i productes protegits contra modificacions i s'ha d'assegurar de la seguretat tècnica i fiabilitat dels processos realitzats per ells.

- Cal aplicar un procediment i registre de gestió de canvis per a versions, modificacions i correccions de software.
- La integritat dels sistemes de l'ens han d'estar protegits contra virus, software maliciós i software no autoritzat.
- Els materials utilitzats en els sistemes de l'ens s'han de gestionar de manera segura per protegir -los de danys, robatoris, accessos no autoritzats i obsolescència.
- S'han de protegir contra la obsolescència i el deteriorament, els materials utilitzats durant el temps en què s'hagin de conservar els registres.
- S'han d'implementar i establir els procediments per a les funcions administratives i de confiança que impacten a la provisió dels serveis.
- L'ens ha d'aplicar procediments per assegurar-se del següent:
    - Els desplegaments de seguretat que estan disponibles s'apliquen en un temps raonable.
    - No s'apliquen desplegaments de seguretat que introdueixen vulnerabilitats o inestabilitats majors que els beneficis que puguin aportar.
    - Es documenten les raons per les quals no d'aplicat un desplegament de seguretat.

Seguretat de les xarxes: L'ens ha de protegir la seva xarxa i els seus sistemes dels atacs.

- L'ens mantindrà tots els sistemes que són crítics per a l'operació de l'ens en una o més zones segures.
- L'ens ha de sotmetre's o realitzar un escàner de vulnerabilitat periòdic en adreces IP publicades i privades identificades per l'ens i registrar proves que cada persona o entitat realitzava cada escaneig de vulnerabilitat amb les habilitats, les eines, la competència, el codi ètic i la independència necessari per proporcionar un informe fiable.
- L'ens s'ha de sotmetre a una prova de penetració en els seus sistemes en la instal·lació i després de la infraestructura o les actualitzacions o modificacions de les aplicacions que determini l'ens com a significatives. L'ens registrarà proves que cada prova de penetració va ser realitzada per una persona o entitat amb les habilitats, les eines, la competència, el codi ètic i la independència necessàries per proporcionar un informe fiable.

Gestió d'incidents: S'ha de controlar l'activitat del sistema relacionada amb l'accés als sistemes informàtics, l'ús de sistemes informàtics i les sol·licituds de servei.

- Les activitats de seguiment haurien de tenir en compte la sensibilitat de qualsevol informació recollida o analitzada
- Les activitats anormals del sistema que indiquen una possible vulneració de seguretat, inclosa la intrusió a la xarxa de l'ens, s'han de detectar i informar com a alarmes.
- Els sistemes de TI de l'ens han de supervisar els següents esdeveniments:
    - Posada en marxa i apagada de les funcions de registre; i

- Disponibilitat i utilització dels serveis necessaris amb la xarxa de l'ens.

- L'ens ha d'actuar de manera oportuna i coordinada per respondre ràpidament a incidents i limitar l'impacte de les violacions de la seguretat. L'ens ha de designar personal de rol de confiança per fer un seguiment de les alertes de esdeveniments de seguretat potencialment crítics i garantir que es registrin incidents rellevants d'acord amb els procediments de l'ens.
- L'ens ha d'establir procediments per notificar a les parts apropiades d'acord amb les normes reguladores aplicables de qualsevol incompliment de la seguretat o pèrdua d'integritat que tingui un impacte significatiu en el servei de confiança prestat i en les dades personals mantingudes en ell, dins de les 24 hores posteriors al moment en que s'identifica l'incompliment.
- Quan l'incompliment de la seguretat o pèrdua d'integritat pugui afectar negativament a una persona física o jurídica a la qual s'ha prestat el servei fiduciari, l'ens també notificarà a la persona física o jurídica l'incompliment de la seguretat o la pèrdua d'integritat sense demora indeguda .
- S'han de controlar els sistemes de l'ens, inclosa la supervisió o la revisió periòdica dels registres d'auditoria per identificar evidències d'activitat maliciosa que impliquen mecanismes automàtics per processar els registres d'auditoria i personal d'alertes de possibles esdeveniments de seguretat crítics.
- L'ens abordarà qualsevol vulnerabilitat crítica que no s'hagi tractat prèviament pel mateix, dins del termini de 48 hores després del seu descobriment. Si això és efectiu en funció de l'efecte en termes de costos, l'ens ha de crear i implementar un pla per mitigar la vulnerabilitat o documentarà la base per la qual la vulnerabilitat no cal ser tractada.
- S'han d'utilitzar els procediments d'informació i resposta dels incidents de manera que es minimitzi el dany causat per incidents de seguretat i mal funcionament.

Alineació amb el Pla de continuïtat de negoci del Consorci AOC: L'ens ha de tenir definit i mantenir un pla de continuïtat que promulgarà en cas de desastre.

Compliment legal i normatiu: L'ens s'ha d'assegurar que opera dins el marc legal aplicable.

- Procediment de compliment de marc legal on es pugui demostrar com es gestiona el marc legal.
- L'ens s'ha d'assegurar que els serveis són accessibles a persones amb discapacitat.
- Compliment del marc legal vigent en protecció de dades personals. Gestió de la identificació:

Gestió del canvi: Procediment transversal on es planifiquin els canvis, es registrin i es dugui un seguiment.

5.4.3.2 Les pautes a seguir per l'auditoria virtual seran:

- Fer un mostreig dels certificats personals generats, entre un 5% i un 10% del total.
- Fer un mostreig dels certificats de dispositiu i aplicació generats (casos d'ER T-CAT i ens subscriptor), entre un 6% i un 10%.

- Sol·licitar al responsable del servei la documentació del mostreig per a analitzar.
- L'auditoria haurà de comprovar que les dades del certificat generat són les mateixes que el certificat sol·licitat o que el DNI o altres documents identificatius. En els casos de full de lliurament de T-CAT es comprovarà que estan degudament signats, arxivats.
- Comprovar la seguretat del tractament de dades personals en compliment de la legislació vigent.

5.4.4 Documentació a lliurar

Per a cada ER auditada, es lliurarà un informe d'auditoria segons el format definit prèviament entre el proveïdor i el Consorci AOC que tindrà una estructura similar als informes d'exemple que es distribueixen juntament amb aquest plec als annexos 2 al 5.

Tota la documentació i comunicacions estaran redactades en català normalitzat.

Aquests informes s'aniran lliurant de forma individual després de la realització de l'auditoria en el termini indicat al punt "5.5 a Termini de lliurament del checklist i evidències d'auditoria". Tots aquests lliuraments seran validats pel Consorci AOC a les fases pertinents i formaran part de l'acta d'acceptació parcial corresponent.

El Consorci AOC haurà de rebre per part de l'adjudicatari, el ***Checklist* de seguiment, les evidències associades i l'informe d'auditoria** tot indicant quines són les no conformitats trobades i les evidències que ho demostren en el termini màxim indicat a "5.5 1-bb Termini de lliurament d'informes" després de l'execució de l'auditoria, per a la seva avaluació i gestió diligent.

A part dels informes d'auditoria de cada ER, es realitzarà un altre informe amb un resum de la visió global del grau de compliment dels procediments de les ER, on s'inclouran taules i gràfics que permetin detectar fàcilment els punts que en general han estat més problemàtics, al final de cada any de servei.

Tota la documentació generada durant l'execució del contracte, incloent els documents de treball i les evidències recollides, seran propietat del Consorci AOC, i l'adjudicatari no podrà facilitar-la a tercers. Aquesta documentació s'anirà guardant a les carpetes de xarxa del Consorci AOC.

Els informes d'auditoria que es considerin "incomplets" per part del Consorci AOC s'hauran de repetir, excepte en el cas que es pugui demostrar que la ER no ha complert amb l'obligació d'oferir de forma oberta tota la informació necessària a l'auditor. Per evitar això es recomana realitzar una bona planificació i conscienciació als ens a la primera fase de l'auditoria

5.4.5 Finalització de l'auditoria

A la recepció de les correccions per part de cada ER, l'auditor avaluarà la conformitat de les accions executades per garantir la correcció de les desviacions.

S'haurà de tenir especial compte per:

- Establir mesures per controlar el progrés de les no conformitats greus.
- Realitzar les revocacions d'ofici dels certificats emesos de manera errònia. (amb els procediments establerts, comunicació al responsable, etc...).
- En cas que l'ER idCAT no faci el recull dels DNI's caldrà que enviïn el correu de plantilla per a que el subscriptor el porti a l'ER. En cas que no el porti en 90 dies, el

proveïdor haurà de comunicar-ho al Consorci AOC qui procedirà a la revocació d'ofici d'aquell certificat.

Un cop avaluat, l'auditor considerarà tancat el procés d'auditoria.

5.4.6 Eina per a la realització remota d'auditories a les ER

El licitador proposarà una eina, programari o plataforma, per a la realització remota de les auditories. Aquesta eina ha de permetre :

- L'enviament dels qüestionaris per cada tipus d'auditoria a l'entitat receptora.
- La càrrega i custòdia de les evidències que proveeixi l'entitat auditada.
- La càrrega de les preguntes i qüestionaris que el consorci AOC indiqui.
- El seguiment en temps real dels qüestionaris enviats, retornats, pendents... per cada tipus d'auditoria.
- La visualització del cronograma i calendari previst per cada tipus d'auditoria i per cada fase (qüestionaris, informes i al·legacions).

L'adjudicatari posarà a disposició suficients llicències per l'ús de l'eina per part de l'equip d'auditoria. També el llicenciament de l'eina haurà de permetre que es puguin auditar totes les entitats destinatàries d'auditoria per any.

La ubicació dels servidors i les dades d'aquesta eina hauran de complir els requisits de protecció de dades aplicables indicades en aquest document.

5.4.7 La gestió de la seguretat i el compliment normatiu

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.

En concret, apliquen mesures proporcionals pel tractament d'auditoria de les dades que pertanyen als subsistemes "Subsistema d'emissió i revocació de certificats" i "Subsistema de EACAT i MUX" definits en el punt "6.4.10.9 Auditoria externa", apartat Esquema nacional de seguretat.

5.4.7.1 Compliment normatiu i legal

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 i GDPR – General Data Protection Regulation, eIDAS - electronic IDentification, Authentication and trust Services)).

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 determinin 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 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.

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 mínims.

5.4.7.2 Requisits de protecció de dades

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 per cadascun dels àmbits especificats en l'apartat "5.4 Condicions" del present PPT i per tot el cicle de vida de les dades, inclòs el seu bloqueig en compliment de l'establert a la LLOPDiGDD. 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).

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.

5.5 Acords de nivell de servei

El funcionament del servei objecte d'aquesta contractació estarà subjecte a un sistema de control de qualitat exercit pel Consorci AOC, tot seguint els Acords de nivell de servei

a. Termini de lliurament del checklist i evidències d'auditoria
   Màxim 15 dies

b. Termini de lliurament d'informes
   Màxim 15 dies

c. Desviació en el compliment de planificació
   5% de programa d'auditories

Aquesta puntuació és important, ja que a part de ser una mesura de qualitat de funcionament del servei, també pot constituir una causa justificada de rescissió del contracte per part del Consorci AOC.

Sens prejudici del que hi ha descrit en aquest document en el punt 5.2, l'adjudicatari anualment haurà de presentar al Consorci AOC un informe amb un pla de millora per al Consorci AOC resultant de les auditories realitzades.

5.6 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'eficaç implantació dels controls definits.

5.6.1 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 determinin en els diferents àmbits del governament del servei objecte d'aquest lot. 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 format i el contingut mínim de la informació a elaborar per l'adjudicatari en tots els àmbits de governament és el definit en l'Annex 5.

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.

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

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

5.6.1.1 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/clients 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

5.6.2 Òrgans de Gestió

5.6.2.1 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.

5.6.2.2 Reunions de Seguiment.

El gestor del servei de l'adjudicatari i el Cap del Servei del SCD 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 incloses 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.
- 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 proposat en definit en l'"Annex _1_Plantilla Informe Seguiment" que inclou, 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 lot. Nombre de consultes realitzades (per tipologia, telèfon, correu, etc,.).
- Millores aplicables al servei de certificació digital.
- 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.

5.7 Devolució del servei

Un cop finalitzat el contracte l'adjudicatari haurà de garantir que ha complert amb tots els compromisos establerts.

A la finalització del servei, l'adjudicatari haurà de presentar la següent documentació al Consorci AOC:

- Informe del mostreig d'entitats de registre auditades durant els últims dos anys del servei.
- Tancament d'informes d'auditoria en un termini previst màxim d'acord al definit al punt d'ANS per aquesta tipologia després de la finalització del servei.
- Llistat actualitzat de la planificació d'auditories a ens subscriptors (auditories no realitzades).
- Llistat actualitzat de comunicacions d'auditories a ens subscriptors (auditories planificades ja comunicades).
- Informe final de conclusions (classificat per tipus d'ER) des de l'últim informe final de conclusions fins a la finalització del servei.
- Informe on hi consta l'avaluació de la conformitat de les accions executades per cada ens subscriptor per garantir la correcció de les desviacions detectades i la identificació d'aquelles accions que no han estat avaluades per l'adjudicatari.

L'adjudicatari haurà de retornar tota la informació confidencial propietat del Consorci AOC, així com la generada a partir de la prestació del servei.

6 Lot 3: SERVEIS DE CERTIFICACIÓ DIGITAL

6.1 Descripció

El Consorci AOC és 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 electrònic al sector públic de Catalunya i amb els seus estatuts.

D'acord amb aquesta competència i en relació a l'objecte d'aquest contracte, s'ha de considerar al Consorci AOC, a tots els efectes, com a Prestador qualificat de serveis de certificació.

En relació a l'àmbit dels Serveis de Certificació Digital i aquells d'altres que en són connexos, vinculats o relacionats, estem davant d'uns serveis d'alta criticitat i complexitat, amb moltes particularitats, una gran quantitat d'usuaris consumint els serveis de manera concurrent, així com una important dependència estratègica amb els serveis digitals dels ens i organismes públics de l'àmbit català usuaris dels serveis.

6.1.1 Catàleg de serveis objecte del contracte

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

6.1.1.1 Serveis a preu unitari i manteniment d'aplicacions informàtiques

Es consideren Serveis sota demanda amb un cost unitari: són els serveis associats a elements tangibles (físics) i no tangibles (digitals) establerts al catàleg de serveis del Consorci AOC, a un cost unitari.

Sota aquestes categories s'inclou el següent catàleg de serveis:

Concepte	Descripció breu
Adquisició de suports criptogràfics (targetes)	Disseny T-CAT estàndard
Servei d'emissió ordinària de suports criptorgràfics (inclou enviament a l'ens sol·licitant)	T-CAT estàndard
Servei d'emissió urgent de suports criptorgràfics (T-CAT Estàndard i inclou enviament urgent a l'ens sol·licitant)	Disseny personalitzat (només gravar xip)
Servei d'emissió urgent de suports criptorgràfics (disseny personalitzat i inclou enviament urgent a l'ens sol·licitant)	T-CAT estàndard
Serveis de programació	Preu/hora programador

Les volumetries per cada servei i any, són les indicades al plec de clàusules administratives.

6.1.1.2 Serveis a tant alçat

Inclou totes les despeses generals necessàries per garantir el bon funcionament del servei amb un volum de la demanda dels serveis de fins a 700.000 certificats vigents per a usuaris únics independentment de l'entitat de certificació emissora, així com els certificats d'aplicació, personals i infraestructura i aquells inclosos en el catàleg de certificats en cada moment, i que no impliquin manipulació directe per part de l'adjudicatari categoritzada en el serveis a preu unitari.

Concretament:

- El finançament de les despeses en maquinari i programari, de posada en marxa, de transició, d'optimització i de devolució del servei (si escau). En concret:
  - La provisió de dispositius criptogràfics HSM per l'entorn de les entitats de certificació segons especificat al punt 6.4.3.4.3.
  - La provisió de les eines de observació dels Acords de Nivell de Servei. En particular de l'eina per l'observació del l'ANS d'emissions i provisió de serveis (punt 6.5.2) i de l'eina per l'observació dels ANS de capacitat i disponibilitat (punts 6.5.2.4 i 6.5.2.3).
- Durant la fase de transició inclou l'adaptació i/o integració d'interfícies, web, portals, infraestructura i EERR avançades.
- Durant la fase de transformació i optimització, inclou la millora de les interfícies de les aplicacions d'usuari final.
- El servei de suport de 2on i 3er nivell adreçat a subscriptors i operadors.
- Manteniment de la documentació associada al servei, manuals, faq's, procediments, etc..
- Les auditories i altres avaluacions periòdiques a que s'hagi de sotmetre el servei.
- L'operació de l'Entitat de Registre T-CAT del consorci AOC segons definit en el punt 6.4.6.
- La generació de paquets de certificats de proves amb dades estàndards.
- La generació de certificats de preproducció sol·licitats.
- L'homologació d'impressores, targetes criptogràfiques i programaris associats.
- La incorporació de fins a dos (2) perfils de certificat addicional per any segons establert al punt 6.4.3.2. (inclou la redacció, implantació i reconeixements i totes les tasques associades)
- La gestió dels reconeixements dels serveis de certificació.
- Facturació dels certificats i control de la facturació.
- Despeses de funcionament ordinari, de gestió operativa i explotació del servei, incloent específicament:
  - Emissió de factures als subscriptors i seguiment
  - Gestió dels estocs de targetes, papereria i material fungible, inclosa la distribució a les entitats de registre
  - Enviament dels certificats
  - Adquisició del material fungible i de papereria necessari
  - Totes les tasques necessàries per al funcionament del servei
- Adequació al marc normatiu vigent en cada moment així com les traduccions necessàries.
- La creació de fins a 20 noves ER IDCAT segons les condicions definides al punt "6.4.5 Model de registre idCAT certificat". Inclou la posada en marxa (sense desplaçament).
- La creació de fins a 3 noves ER T-CAT estàndard amb impressora de targetes amb suport criptogràfica i segons les condicions definides al punt "6.4.4.1 Entitat de registre T-CAT". Inclou la posada en marxa estàndard amb suport presencial.
- El suport a fins a 15 formacions virtuals d'operadors d'ER idCAT o TCAT. Les sessions seran amb un màxim de 25 alumnes, segons les condiciones definides al punt 6.4.8.

- El suport a fins a 5 formacions presencials d'operadors ER T-CAT. Les sessions seran amb un màxim de 30 alumnes i durada de fins a 4 hores, segons les condicions definides al punt 6.4.8.

Els següents serveis no són objecte d'aquest contracte:
- El servei de suport de primer nivell.
- La compra de les impressores de plàstic i criptogràfiques per a les entitats de registre, els recanvis ni el servei de manteniment d'aquest maquinari.

6.2 Funcions

L'adjudicatari del present lot haurà de permetre al Consorci AOC prestar els serveis descrits a les Polítiques de Certificació i la Declaració de Pràctiques de Certificació del Consorci AOC, publicades a http://epscd.aoc.cat/regulacio; i a les condicions generals i específiques a l'apartat funcions del consorci AOC:

https://www.aoc.cat/serveis-aoc/condicions-prestacio-serveis-aoc/

Condicions generals del Consorci AOC (versió del 13/03/2019):

https://www.aoc.cat/wp-content/uploads/2015/11/condicions-generals-de-prestacio-de-serveis_13032019.pdf

Condicions específiques Er-T-CAT (punt 4, versió del 4/9/2015):

https://www.aoc.cat/wp-content/uploads/2015/11/Condicions-espec%C3%ADfiques-dels-Serveis-AOC_ER_T-CAT.pdf

Condicions específiques ER-idCAT (versió del 23/6/16):

https://www.aoc.cat/wp-content/uploads/2015/11/Condicions-espec%C3%ADfiques-dels-Serveis-AOC_ER_idCAT.pdf

Un extracte de les funcions que el Consorci AOC trasllada a l'adjudicatari i que s'enumeren en les condicions específiques com a prestador del servei són:

- Emetre, lliurar, administrar, suspendre, revocar i renovar certificats en els casos i pels motius descrits a la Declaració de Pràctiques de Certificació de les Entitats de Certificació de la Jerarquia Pública de Certificació de Catalunya.
- Executar els serveis amb els mitjans tècnics i materials adequats, i amb personal que compleixi les condicions de qualificació i experiència establertes a la Declaració de Pràctiques de Certificació de es Entitats de Certificació de la Jerarquia Pública de Certificació de Catalunya
- Complir els nivells de qualitat del servei, de conformitat amb el que s'estableix a la Declaració de Pràctiques de Certificació de les Entitats de Certificació de la Jerarquia Pública de Certificació de Catalunya, en els aspectes tècnics, operatius i de seguretat.
- Notificar al subscriptor, com a mínim amb dos mesos d'antelació a la data d'expiració dels certificats, la possibilitat de renovar-los, així com la suspensió, habilitació o revocació dels certificats.
- Comunicar a les terceres persones que ho sol·licitin l'estat dels certificats, d'acord amb el que s'estableix a la Declaració de Pràctiques de Certificació de les Entitats de Certificació de la Jerarquia Pública de Certificació de Catalunya per als diferents serveis de verificació de certificat.
- Emetre un certificat per a cada operador nomenat per l'ens usuari després de l'aprovació de la sol·licitud del certificat corresponent.

- Impartir la necessària formació al personal de l'ens usuari en especial als operadors, per a l'execució de les seves tasques.
- Comunicar a l'ens usuari qualsevol canvi que es produeixi en les Polítiques de Certificació i en la Declaració de Pràctiques de Certificació de les Entitats de Certificació de la Jerarquia Pública de Certificació de Catalunya.
- El Consorci AOC garanteix que les claus privades de les Entitats de Certificació de la Jerarquia Pública de Certificació de Catalunya, utilitzades per emetre certificats, no ha estat compromesa, llevat que el Consorci AOC hagi comunicat el contrari, d'acord amb el que s'estipula a la Declaració de Pràctiques de Certificació de les Entitats de Certificació de la Jerarquia Pública de Certificació de Catalunya.

L'adjudicatari haurà de posar a disposició les infraestructures necessàries per la correcta prestació dels serveis d'acord a uns determinats requisits (punt **¡Error! No se encuentra el origen de la referencia.**) i condicions (punt 6.4) exposats en el present document, regits per uns Acords de nivell de servei determinats (punt 6.5), amb un determinat model de seguiment del servei (punt 6.6) i en les fases proposades (punt 6.4.2, 6.7 i 6.8).

A continuació es presenta una estructuració de les funcions i responsabilitats de l'adjudicatari i del Consorci AOC en un 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 lot (punt 6.6) se sustenta 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.

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

6.2.1 Estructura de responsabilitats de l'adjudicatari

L'estructura de responsabilitats i competències mencionada es concreta en els següents responsables. L'equip de responsables haurà de disposar del dimensionament, la formació i els mitjans adequats per a desenvolupar les funcions i responsabilitats assignades.

Per part de l'adjudicatari:

- Responsable de compte: És la figura de referència en el marc del contracte entre el Consorci AOC i l'adjudicatari, i serà el darrer responsable de la prestació del conjunt de serveis i projectes de l'adjudicatari. 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. Ha de ser garant de l'existència dels mecanismes de relació en la seva organització per portar a terme els acords presos entre el Consorci AOC i l'adjudicatari.

- Responsable de serveis: El proveïdor assignarà un responsable, les principals responsabilitats 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: 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. Serà responsable de que el Consorci AOC rebi els informes de gestió acordats, tant amb indicadors econòmic-financers com d'altres, així com de realitzar el seguiment del model econòmic acordat amb l'adjudicatari.

- Responsable Jurídic: Serà l'interlocutor principal amb el Consorci AOC en matèria jurídico-legal pels serveis prestats per l'adjudicatari.

- 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 ens 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: És el responsable de coordinar i harmonitzar l'aplicació de l'arquitectura corporativa en els sistemes d'informació i serveis a construir o mantenir pel proveïdor. Les seves principals responsabilitats són:
    - Vetllar pel compliment dels principis associats als diferents dominis, i pel compliment dels estàndards d'arquitectura corporativa TIC.
    - Proposar noves arquitectures TIC alhora que es mantenen i/o evolucionen les existents (funció d'innovació).
    - Vetllar per la coherència en l'aplicació de l'arquitectura corporativa TIC.
    - Identificar els components reutilitzables i promocionar-ne tant la generació com l'ús.

- Proporcionar un mecanisme de control, fonamental per assegurar el compliment efectiu dels estàndards d'arquitectura corporativa TIC.

- 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 nivell, del Consorci AOC; i també de 2n i 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: Serà responsable de:
  - Assegurar l'existència d'un pla de qualitat pels serveis i aplicacions.
  - L'assegurament de la qualitat.
  - La verificació de l'execució del control de la qualitat.

- Responsable de Seguretat: Serà responsable de:
  - Actuar com a enllaç entre l'adjudicatari i els diferents agents implicats (Consorci AOC, CESICAT) 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 el CESICAT 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...).
  - Assegurar que tot el personal del proveïdor que hagi de tractar dades o sistemes de tractament de dades de nivell sensible o superior signin un Acord de Confidencialitat Individual. El Consorci AOC podrà auditar aquest aspecte.
  - 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 Continuïtat: 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 exigit pel Consorci AOC.
    - Assegurar la informació regular al consorci AOC segons els terminis marcats, de tot allò relacionat amb la Continuïtat 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.

6.2.2 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: Serà el responsable de presentar la planificació, abast i metodologia d'execució dels diferents plans de transició del servei. Impulsarà. 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 de Certificació Digital

- Cap de Projecte de l'Àrea de Tecnologia
- Responsable d'Assessorament Jurídic de Serveis del Consorci AOC.
- Responsable del sistema del Consorci AOC
- Representant de la Direcció

6.2.3 Recursos tecnològics proveïts pel Consorci AOC

- Maquinari i programari:
  - HSM's jerarquia PRO i CONT i offline. Amb model de seguretat a transferir.
  - Documentació jurídica
  - Codi de les aplicacions de les Entitats de Registre T-CAT i idCAT
  - Maquinari de les ER : impressores i lectors
  - Stock de targetes criptogràfiques.
  - Configuració de la PKI actual (EJBCA).
- Repositoris de informació:
  - Carpetes de Sharepoint del Consorci AOC per documentació del servei.
  - GIT pel codi.
- Eines control ANS:
  - ANS disponibilitat: ISM
  - ANS evolutius i peticions del servei : JIRA del Consorci AOC
  - ANS suport: Zendesk del Consorci AOC

El Consorci AOC durant la vigència del contracte es reserva el dret de canviar els recursos tecnològics descrits en aquest punt.

6.2.4 Recursos tecnològics a proveir per l'adjudicatari

- Entorns per allotjament de les claus i aplicacions:
  - Entorn de Producció
  - Entorn de contingència
  - Entorn de Preproducció
- Maquinari, programari i comunicacions:
  - Necessari per prestació del serveis objecte del contracte.
- Eines de control ANS:
  - ANS disponibilitat: Opensearch o equivalent
  - ANS indicadors de servei : OpenSearch o equivalent.
  - ANS disponibilitat i capacitat : OpenSearch o equivalent.

6.3 Requisits

6.3.1 Requisits personals

Les tasques a desenvolupar en aquest lot s'han calculat a partir de la incorporació (en diferent percentatge) dels perfils següents:

- Responsable
- Tècnic

- Programador

Per poder oferir tots els serveis objecte d'aquest lot en un escenari de consum màxim, és a dir, de tots els serveis previstos a "Preu unitari i desenvolupament i manteniment d'aplicacions informàtiques" i també els de "tant alçat", s'han calculat els volums d'hores per any i categoria definides al punt B1 del plec de clàusules administratives.

En tots els casos, es calcula sobre unes 1.700 hores/any persona (inclou, per tant, es tenen en compte els dies de baixa i absències).

El personal adscrit al servei, en conjunt, ha de disposar dels coneixements suficients acreditats, tant a nivell tècnic pràctic com d'idiomes (domini del català (nivell C), castellà i l'anglès), que assegurin la correcta interpretació de procediments i normes de seguretat, fet que ha de permetre una correcta aplicació d'aquests coneixements.

El personal que l'adjudicatari destini a aquest servei haurà de reunir totes les condicions estipulades per la normativa actualment vigent.

El Consorci AOC pot refusar i/o sol·licitar el canvi d'interlocutor o responsables de projecte. En aquest cas, l'adjudicatari ha de reemplaçar al treballador per un altre suficientment capacitat per dur a terme la tasca encomanada. Els costos derivats d'aquesta incidència aniran a càrrec de l'adjudicatari.

El Consorci AOC es reserva el dret de no acceptar el personal que desenvolupi la seva tasca sense una capacitació suficientment o un comportament incorrecte.

Caldrà presentar una taula de correlació entre els mitjans requerits al punt "6.2.1 Estructura de responsabilitats de l'adjudicatari" i els presentats per part de l'adjudicatari.

L'adjudicatari s'ha de fer càrrec de tots els materials i útils per a la correcta execució dels serveis encomanats, degudament identificats com de la seva propietat.

El Responsable de serveis proposat per l'adjudicatari haurà de disposar d'un número de telèfon que permeti la seva localització en jornada laboral del calendari laboral de Barcelona, per part del personal responsable del Consorci AOC.

Per tal de poder conèixer la qualificació professional, el licitador presentarà el currículum professional dels candidats que proposin per aquests perfils. El licitador justificarà documentalment la qualificació professional del personal destinat amb la presentació de la documentació compulsada que es detalla a continuació: targeta d'identitat professional i títols professionals.

En cas de baixa de qualsevol dels membres de l'equip, l'adjudicatari haurà de substituir-lo en menys de 15 dies laborables d'acord amb els responsables del Consorci AOC. Qualsevol canvi en un dels membres de l'equip a instàncies de l'adjudicatari haurà de ser pactat amb el Consorci AOC, que haurà de validar tant la baixa com el currículum de la nova persona a incorporar. Si el canvi és a instàncies de l'adjudicatari, caldrà acordar el calendari de canvi amb el Consorci AOC per tal de minimitzar l'impacte en els desenvolupaments en curs. Resten fora d'aquest compromisos els períodes de vacances i permisos de tots els membres de l'equip.

El Consorci AOC realitzarà, si s'escau, entrevistes a les persones de l'equip de projecte proposat i, si és necessari, demanarà alternatives a les persones presentades.

El Consorci AOC es reserva el dret a demanar el canvi de qualsevol dels membres de l'equip sense necessitat de justificació amb una antelació de 20 dies naturals a la data de substitució.

El Consorci AOC es reserva el dret a demanar una declaració personal de cada un dels auditors per garantir la seva formació i coneixements.

L'adjudicatari haurà de presentar al Consorci AOC, la fitxa personal de cada responsable, tècnic i programador que proposi per les funcions definides, on hi constarà:

- nom i cognoms
- qualificació educativa i categoria professional
- experiència i formació
- avaluació de la competència: coneixements de la tecnologia i marc legal aplicable.
- seguiment de l'acompliment
- data de l'actualització més recent de cada registre

6.3.2 Catàleg de certificats del Consorci AOC

El catàleg de certificats digitals que el Consorci AOC ofereix actualment als usuaris del Servei de Certificació Digital (SCD), mitjançant els serveis que prestarà l'adjudicatari d'aquest lot, és el que es pot consultar al punt "1.1.1. Tipus i classes de certificats" de la Declaració de Pràctiques de Certificació publicada al web del servei a epscd.aoc.cat.

Correspondència a les categories de Serveis eIDAS:

- TrustedList/SvcInfoExt/ForeSignatures : T-CAT personals i idcat.
- TrustedList/SvcInfoExt/ForeSeals : Segells electrònics i Dispositiu aplicació.

A part de les categories eIDAS també es realitzen certificats d'operador tant idCAT com T-CAT.

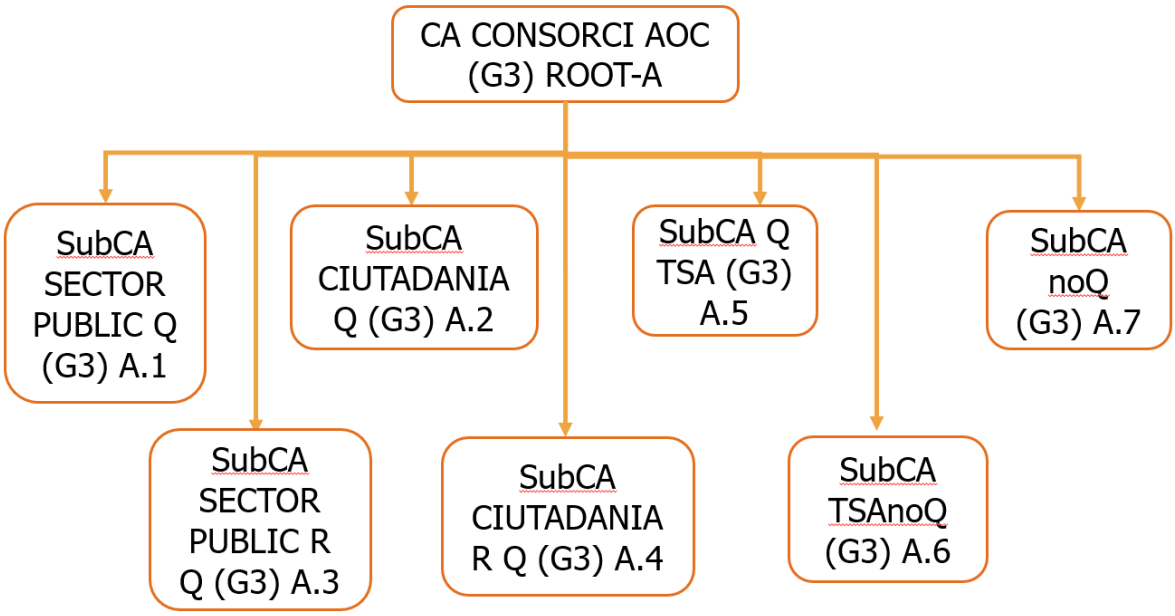
L'històric de volumetries del servei es pot consultar al document Annex 6.

El Consoci AOC es reserva el dret de modificar el seu catàleg de certificats quan ho consideri oportú.

6.3.3 Explotació de la Jerarquia dels Serveis Públics de Certificació de Catalunya

La següent figura mostra l'estructura de l'actual Jerarquia dels Serveis Públics de Certificació de Catalunya en l'àmbit d'explotació d'aquest contracte i que està formada per :

- Una Entitat de Certificació arrel (Root CA), que és l'EC-ACC,
- La jerarquia de la primera generació estava formada per cinc Entitats de Certificació de 2n nivell (l'EC-GENCAT, l'EC-AL, l'EC-UR, l'EC-Parlament i l'EC-IDCAT) i dues Entitats de Certificació de 3r nivell (l'EC-SAFP i l'EC-URV). Aquestes entitats estan finalitzades.
- La jerarquia de la segona generació formada per dues Entitats de Certificació de 2on nivell (l'EC-SECTORPUBLIC i l'EC-CIUTADANIA) que concentren totes les emissions dels tipus de certificats que formen part del catàleg de certificats ofert pel Consorci AOC.
- La jerarquia de tercera generació es va emetre a 2022 i està formada per set entitats de certificació subordinades i una Entitat de Certificació arrel. En l'àmbit d'aquest contracte hi ha la nova arrel i les subCAs A1, A2, A5, A6 i A7.



6.3.3.1 Infraestructura de Hosting i Maquinari / Continuïtat de serveis de jerarquia i claus

La infraestructura de l'actual jerarquia d'Entitats de Certificació (en endavant, ECs) està desplegada en els següents entorns:

Producció:

- EC arrel (Offline, desconnectada d'internet): en un "CPD" (de l'adjudicatari actual, situat a la provincia de Barcelona).
- ECs subordinades: en alta disponibilitat, en un "CPD" (de l'adjudicatari actual, situat a la província de Barcelona).

De contingència:

- ECs arrel i subordinades: en el CPD primari del Consorci AOC, a la província de Barcelona, i operat per l'adjudicatari actual.

De Preproducció (i Integració):

- EC arrel i subordinades de preproducció: en un CPD titularitat de l'adjudicatari actual.

Els dispositius actuals que donen servei compleixen el marc normatiu aplicable i estan certificats com a FIPS 140-2 nivell 3 o EAL4+. Aquests equips s'han mantingut en tot moment i, en alguns casos mentre els contractes de suport del fabricant ho han permès, sota garantia del fabricant. El detall exacte dels dispositius es pot consultar a l'ANNEX 11 sobre l'inventari d'actius (maquinari i llicències contractades).

Els actuals custodis de les targetes que permeten l'operació dels dispositius criptogràfics associats a aquestes EC's són personal directiu o amb rols de Seguretat assignats en el Servei de Certificació del Consorci AOC i també personal de l'adjudicatari actual.

6.3.3.2 Aplicació PKI actual de la de la Jerarquia dels Serveis Públics de Certificació de Catalunya

L'aplicació que suporta a la Infraestructura de clau pública (PKI) de l'actual Jerarquia dels Serveis Públics de Certificació de Catalunya ofereix les funcionalitats i el rendiment que s'exposen a continuació:

6.3.3.2.1 Emissió de Llistes de Revocació de Certificats (CRL's)

Cada Entitat de Certificació (en endavant EC), genera les seves llistes de revocació (en endavant, CRL's, l'acrònim en anglès de Llista de Revocació de Certificats) en les condicions – de periodicitat, vigència, etc. – que s'estableixen a la seva Declaració de Pràctiques de Certificació, publicada a: http://epscd.aoc.cat/regulacio i sempre d'acord a la normativa aplicable.

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

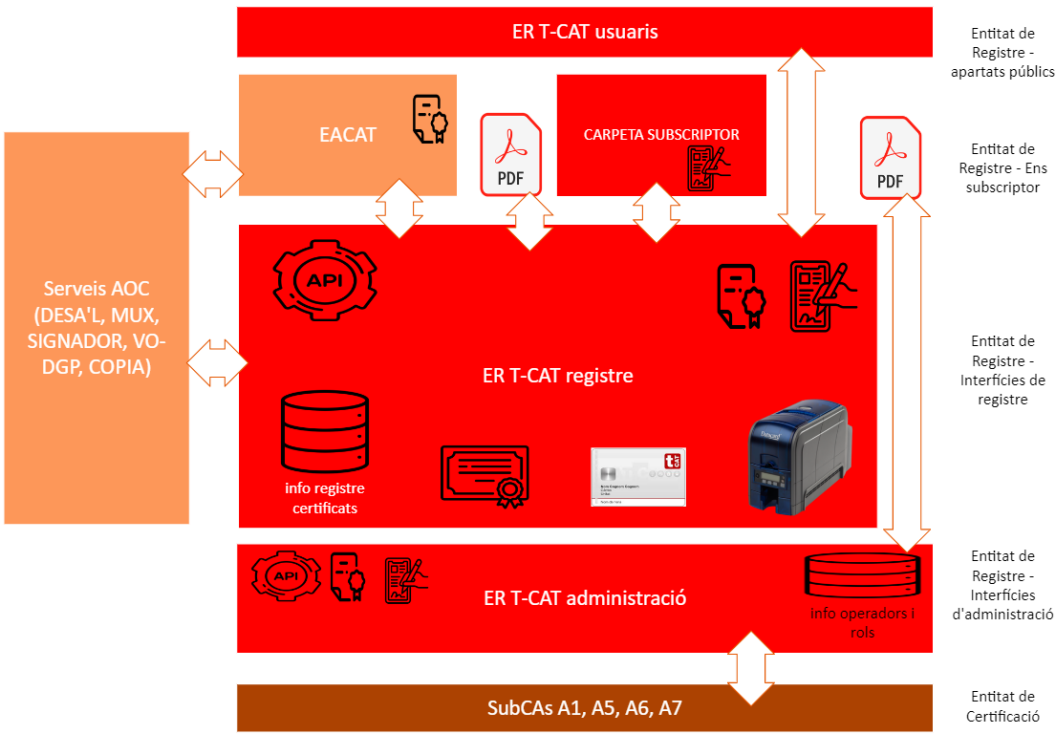
La infraestructura PKI haurà de proveir serveis de validació a través del protocol de Consulta d'Estat de Certificats en Línia (en endavant, OCSP, l'acrònim en anglès de Consulta d'Estat de Certificats en Línia).

Per a cada EC configurada al servei OCSP, es disposa d'una clau amb usos de signatura de respostes OCSP emesa per aquesta EC. Així, permetent que un únic servei pugui donar respostes sobre certificats emesos per totes les EC's de la jerarquia, signades amb una clau de la mateixa EC que va emetre el certificat que es vol validar (tal com fa actualment el servei publicat a: http://ocsp.catcert.cat), el servei és interoperable amb la validació dels certificats SSL que fan els navegadors.

Per a cada EC configurada al servei OCSP, el servei OCSP no podrà respondre l'estat desconegut (UNKNOWN) per certificats que no ha emès, d'acord a la normativa vigent aplicable.

6.3.4 El Servei de Certificació Digital del sector públic català (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 Public. Com a perfils de certificat s'hi inclouen els certificats de signatura electrònica i de segell electrònic.



6.3.4.1 Model de Registre

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 (descrit 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.

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

6.3.4.2 Rols del sistema T-CAT

Els Rols implicats en l'emissió i gestió de certificats T-CAT divideixen en dos pel fet de residir en dos nivells de registre diferent dins del procés d'emissió. Són els "Rols al portal d'operadors de registre i la Carpeta del Subscriptor" i els "Rols web Operadors / Entitat de registre ". Els primers es recullen als documents "FITXA ENS Subscriptor" i els segons al "FITXA ER T-CAT" que es troben al web del consorci AOC a "https://www.aoc.cat/serveis-aoc/catcert-t-cat-administracions/".

6.3.4.2.1 Rols al portal d'operadors de registre i la Carpeta del Subscriptor

Estan definits a la web del Consorci AOC a "https://www.aoc.cat/knowledge-base/quins-tipus-de-rols-hi-ha-a-la-part-del-servei-de-certificacio-digital-a-leacat/".

6.3.4.2.1.1 Responsable del servei de certificació digital

Els responsables del servei de certificació digital són les 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.

6.3.4.2.1.2 Certificador de dades

Els certificadors de dades són les 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.

6.3.4.2.1.3 Sol·licitant de certificats personals o d'entitat

Persona amb autoritat dins de l'ens per sol·licitar l'emissió, renovació, habilitació i revocació de certificats personals o d'entitat (p.e. l'alcalde, un 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.

6.3.4.2.1.4 Sol·licitant de certificats de dispositiu i aplicació

Persona amb autoritat dins de l'ens per sol·licitar l'emissió, renovació, habilitació i revocació de certificats de dispositiu i aplicació (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.

6.3.4.2.1.5 Editor de sol·licituds a EACAT

Els editors de sol·licituds són les persones que poden emplenar, tot i que no signar, sol·licituds d'emissió, renovació, habilitació i revocació de certificats digitals a través d'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:

6.3.4.2.2 Rols web Operadors / Entitat de registre T-CAT

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:

6.3.4.2.2.1 Peticionari

Persona encarregada d'introduir les dades de les sol·licituds dels 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 EACAT o en cas de problemes tècnics que impedeixin fer ús de la plataforma.)

6.3.4.2.2.2 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 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, pro-ves dels ens que sol·liciten certificats, etc.

6.3.4.2.2.3 Generador

Persona encarregada de generar els certificats un cop aprovades les peticions.

6.3.4.2.2.4 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 EACAT, aquest rol desapareix i queda per a casos d'emergència (en què no sigui possible fer servir EACAT).

6.3.4.2.2.5 Dipositari AOC

Operador amb permisos per efectuar el lliurament i la descàrrega de certificats cedits pels ens al Consorci AOC.

6.3.4.2.2.6 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 l'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 enllaç entre l'organització i el Consorci AOC.

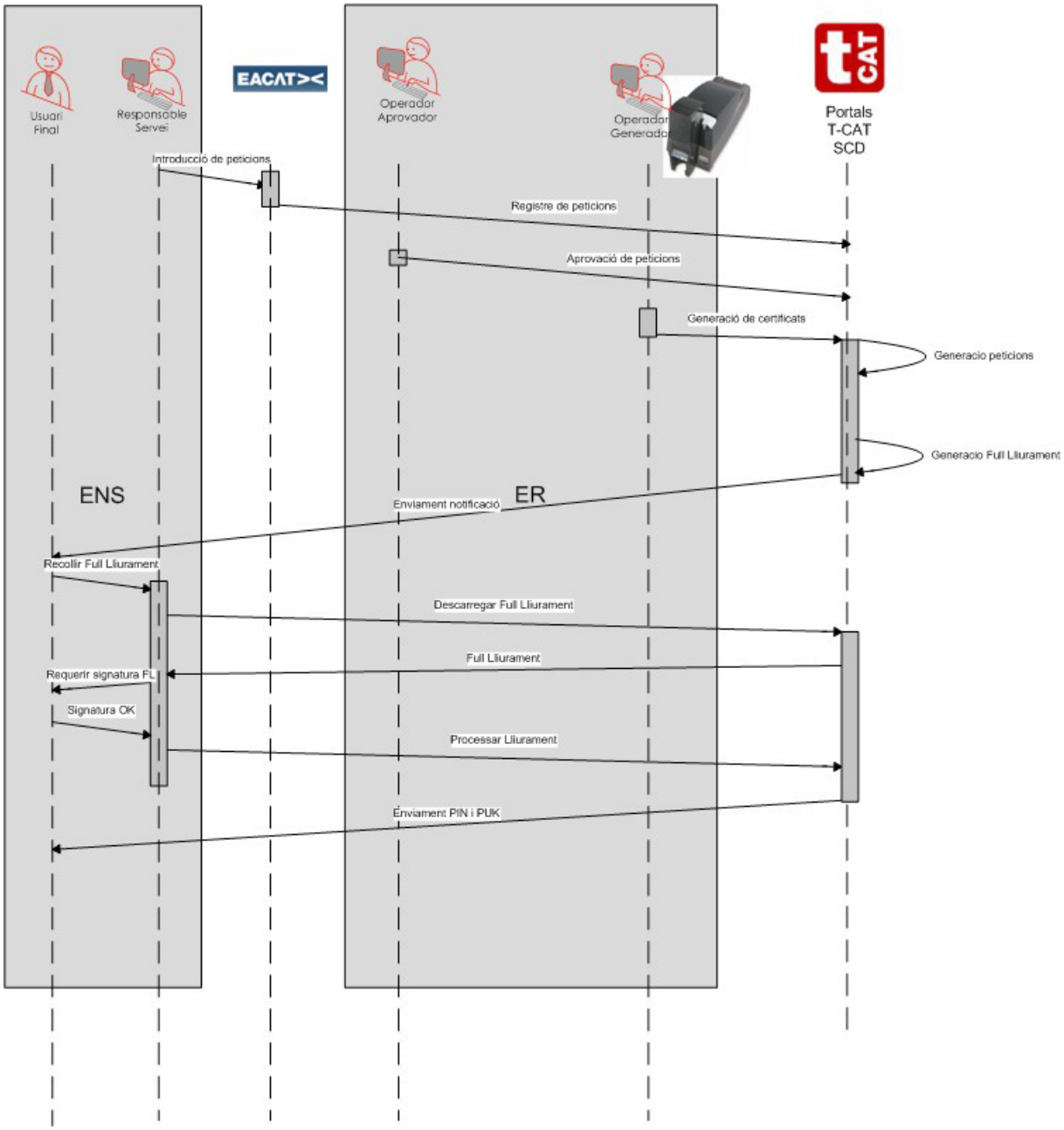
6.3.4.3 El Servei d'emissió de certificats T-CAT

Els procediments operatius de les ER's de T-CAT es troben a l'apartat Qui Sou? Del Servei El Consorci AOC de la web del Consorci AOC.

Mitjançant els següents diagrames de relacions, s'il·lustren els processos d'emissió de certificats digitals en els seus diferents formats (T-CAT i T-CATP). Els esquemes mostren els rols que intervenen i la seva localització física al llarg del procés.

6.3.4.3.1 Procediment d'emissió 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 enviat per correu electrònic:

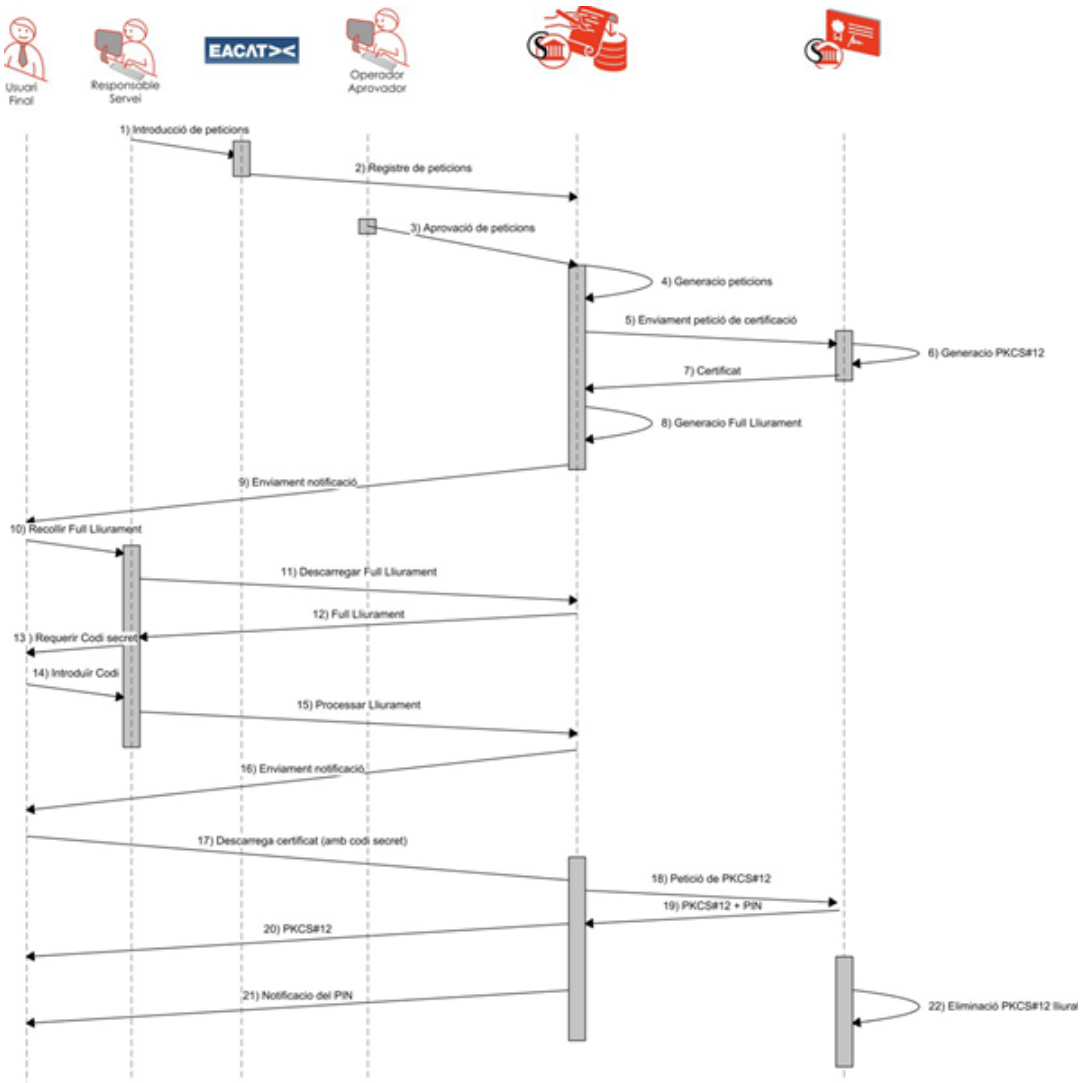


El diagrama de flux pot introduir les variants/excepcions:

- Els certificats de dispositiu servidor o aplicació es generen automàticament pel programari sense la intervenció del Mòdul Generador
- Existeixen variants d'emissió massiva que utilitzen connectors automàtics per a càrrega massiva de dades, consulta d'estats i emissió massiva desatesa, entre d'altres funcionalitats.
- Algunes entitats grans són ER a la vegada i es fan les seves targetes. Es pot donar el cas que no carreguin les peticions al sistema via EACAT, sinó a través dels connectors directament.
- Més informació de mòduls i funcionalitats personalitzades a l'Annex 9.

6.3.4.3.2 Procediment d'emissió T-CAT-P (Programari)

El següent diagrama de flux representa el procediment d'emissió estàndard d'un certificat T-CAT-P en programari amb la sol·licitud a través d'EACAT.



6.3.4.3.3 Dissenys i personalització de targetes

El sistema de Certificació digital T-CAT suporta actualment aquestes categories de dissenys de plàstics de targetes.

6.3.4.3.3.1 Estàndard T-CAT

Disseny de targeta estàndard aprovat pel Consorci AOC. Suporta banda magnètica i impressió de text sense foto, només per la part de davant.

6.3.4.3.3.2 Personalitzat per Ens

Disseny de targeta personalitzat per a cada ens d'acord amb els seus requisits estètics. El format l'acorda cada ens amb el fabricant de targetes i personalitza amb foto. El Consorci AOC, en aquest cas, només genera el certificat al xip criptogràfic.

La relació de quins ens tenen targeta personalitzada es recull a l'annex "Annex_9_Resum_caracteristiques_ERs_TCAT".

6.3.4.3.4 Solució tecnològica per al Servei d'emissió de targetes

El servei d'emissió de certificats i personalització completa de la targeta, en un sol pas, és possible gràcies a una aplicació feta a mida per aquest servei. Aquesta aplicació grava el certificat i personalitza la targeta amb les dades que s'han carregat en el sistema de Registre. És a dir, segueixen el mateix camí de càrrega en el sistema i validació que les dades que s'incorporaran als certificats digitals. D'aquesta manera s'aconsegueix fer de l'emissió i personalització de la targeta un procés atòmic i en un sol pas.

Per gestionar la impressió i els processos associats a través de la impressora criptogràfica, és necessari instal·lar a les estacions de registre que operen el mòdul generador, un programari de client desenvolupat a mida i que requereix una instal·lació específica i l'homologació prèvia de tots els components que composen l'equip. Per aquesta raó, els ordinadors client que utilitzen l'aplicació per les ER's del SCD del Consorci AOC per al mòdul generador són equips dedicats i homologats per tal de garantir que l'aplicació d'emissió funcionarà correctament. Actualment el programari d'emissió és compatible amb les darreres versions de Windows.

Pel que fa a les impressores criptogràfiques, també s'ha homologat cada model d'impressora suportat amb el programari d'emissió i personalització. A més, també s'ha validat la compatibilitat amb cada versió de sistema operatiu i resta de programari. Actualment, l'aplicació és compatible amb les impressores que s'especifiquen en el document d'inventari i en el document de funcionalitats de les EERR adjunts.

6.3.4.3.5 Model de provisió i manteniment del maquinari d'emissió de l'SCD T-CAT

Tal i com s'ha esmentat en els punts anteriors, la complexitat inherent al fet de mantenir una aplicació de generació amb capacitat de generació i alta personalització de la targeta, ha motivat la homologació d'uns equips i components de programari concrets per tal de mantenir el correcte assoliment de l'objectiu funcional. De la mateixa manera, en el seu inici es van proveir els equips per als diferents ens que s'establien com a ER. D'aquesta manera i, en general, s'ha proveït un equip PC, una impressora làser per a la impressió de documentació, si s'escau, i una impressora criptogràfica per al seu ús en l'emissió de certificats de l'SCD T-CAT.

Aquests equips s'han mantingut en tot moment i, en alguns casos mentre els contractes de suport del fabricant ho han permès, sota garantia del fabricant.

Addicionalment, també s'ofereix un servei de manteniment del maquinari i programari de les ER's: actualment el Consorci AOC dóna suport (fins i tot in situ, quan és necessari) al personal tècnic dels ens que operen les ER's. En cas que el maquinari de l'ER hagi estat proveït pel Consorci AOC, també s'ofereixen serveis de manteniment d'aquest (reparació, reposició, etc) en condicions que garanteixen l'acord de nivell de servei pel servei ordinari d'emissió i renovació de certificats compromès amb els usuaris.

6.3.4.3.6 Models de provisió dels suports criptogràfics

Hi ha dos grans models de provisió dels suports criptogràfics en l'SCD T-CAT actual. Són aquests:

6.3.4.3.6.1 T-CAT estàndard

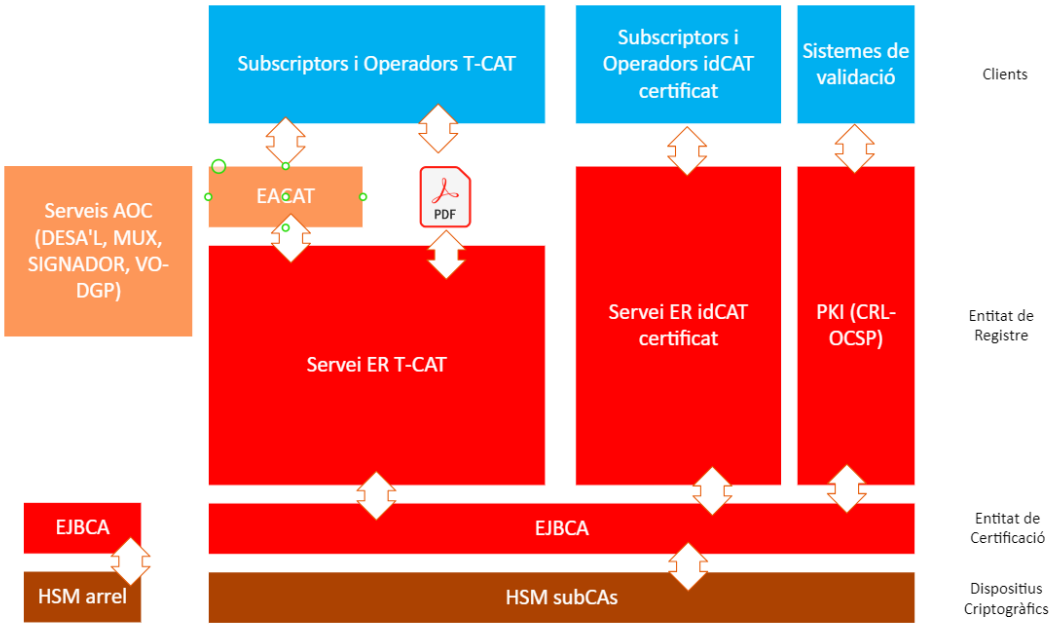
Adquirida pel Consorci AOC directament al fabricant d'acord amb els requisits del Consorci AOC. Aquesta targeta és la que utilitzen la majoria d'ERs col·laboradores dels Consells Comarcals que donen servei a les ERs vinculades assignades al seu àmbit i també per la ER del Consorci AOC. En el cas de les ERs col·laboradores que utilitzen aquest model de targeta, és el Consorci AOC qui els hi envia periòdicament un estoc de targetes per al seu ús.

6.3.4.3.6.2 Targeta personalitzada

Adquirida per cada ER col·laboradora directament al fabricant i d'acord amb les seves especificacions negociades amb el fabricant. Adopta un xip homologat pel Consorci AOC i una personalització de foto, si s'escau.

6.3.4.4 Descripció de components i interfícies de programari del Servei de Certificació Digital (T-CAT i idCAT)

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), respositori documental (DESA'L), aplicacions de signatura (SIGNADOR), servei de digitalització (COPIA), accés a dades de la DGP (VO-DGP), etc..

6.3.4.5 L'Entitat de Registre T-CAT del Consorci AOC

El Consorci AOC opera una Entitat de Registre (en endavant ER) que és la que centralitza les peticions de certificats digitals en targeta criptogràfica de tots els ens que no estan vinculats a una ER Col·laboradora. Des de l'ER del Consorci AOC també es generen alguns certificats amb requisits de validacions més elevats, com són els perfils de representant.

Quan el volum de sol·licituds rebudes supera les 100 targetes, el sistema les permet derivar al fabricant de les targetes per tal que faci la producció massiva del lot i gestioni els corresponents enviaments postals als ens subscriptors. La producció a la fàbrica permet les

mateixes personalitzacions i serveis avançats que s'incorporen des de les estacions de generació de les ER Col·laboradores.

El processat del fitxer de lot es fa a través d'una personalització del programari del mòdul Generador que opera únicament des de l'ER del Consorci AOC. Consta d'un procés d'intercanvi de dades de forma segura i, entre d'altres dades, s'intercanvien les claus públiques a certificar, els certificats un cop emesos, els PINs i PUKs de les targetes per emmagatzemar-los a la carpeta del subscriptor, etc.. Tot el procés de registre per lots informa les mateixes dades al sistema que una emissió normal i, d'aquesta manera, s'aconsegueix que les targetes emeses per lots o des de les estacions de generació, tinguin la mateixa funcionalitat i operativa en la fase del lliurament (carpeta del subscriptor).

6.3.4.6 Gestió documental del Servei de Certificació T-CAT

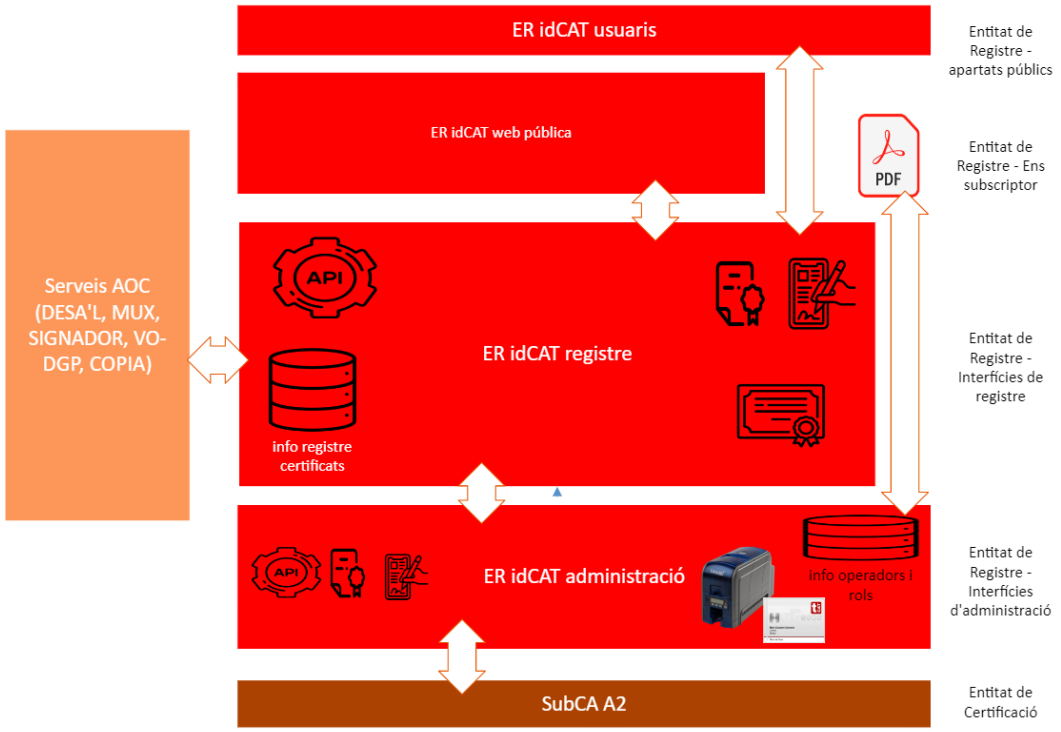
El programari de l'ASCD d'EACAT, que gestiona el tràmit de sol·licitud de certificats T-CAT i les fitxes de subscriptors, s'integra amb el gestor documental del Consorci AOC (anomenat DESA'L) per a la gestió de la documentació derivada del tràmit.

El mòdul ASCD d'EACAT 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 exigit.

6.3.5 El Servei de Certificació Digital per la ciutadania (idCAT certificat)

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:



6.3.5.1 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.

6.3.5.2 La Web dels Operadors

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.

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.

6.3.6 La Web dels Operadors de Certificació o d'administració

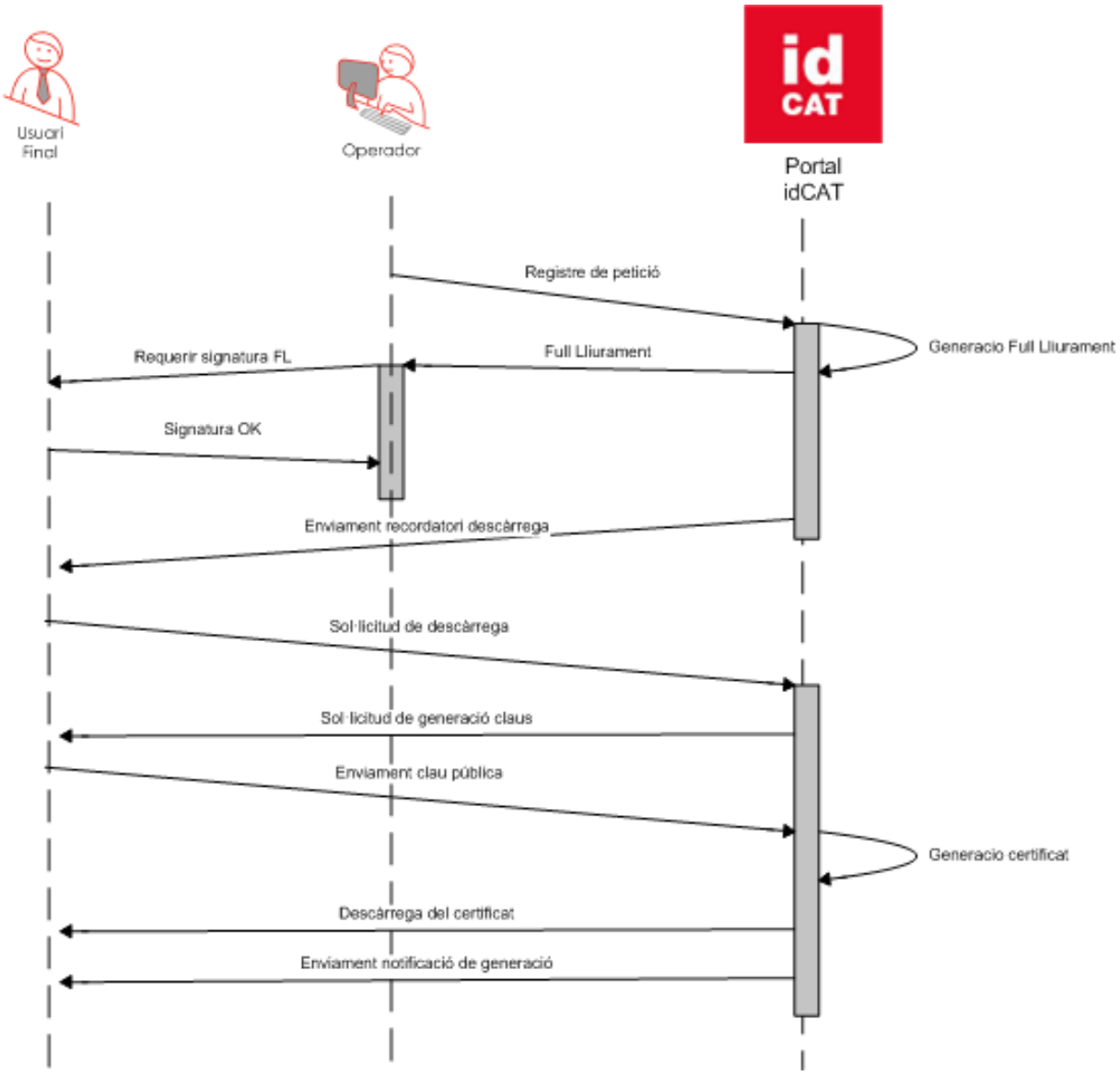
Des d'on es controlen els permisos dels operadors del servei idCAT i es generen els certificats en targeta per a operadors del sistema.

Dimensions ER idCAT:

- Número d'ERs: 393
- Número d'operadors de les ERs idCAT: 4.125

6.3.6.1 Procediment de sol·licitud i emissió idCAT certificat

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.

6.3.6.2 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.

6.4 Condicions

6.4.1 Condicions generals i específiques de Prestació dels serveis objecte del contracte per part del Consorci AOC

L'adjudicatari haurà de oferir els serveis objecte del contracte d'acord a les condicions generals i específiques definides pel Consorci AOC en aquesta documentació:

https://www.aoc.cat/condicions-prestacio-serveis-aoc/

Condicions generals Consorci AOC:

https://www.aoc.cat/wp-content/uploads/2023/06/CON_GENERALS-PRESTACIO-SERVEIS_29062023.pdf

Condicions específiques ER T-CAT:

https://www.aoc.cat/wp-content/uploads/2021/10/CON_especifiques-ER-TCAT_01102021.pdf

Condicions específiques ER idCAT:

https://www.aoc.cat/wp-content/uploads/2024/01/CON_Condicions-especifiques-ER-idCAT_24012024.pdf

Els ANS descrits en les condicions anteriors s'especifiquen en el punt 6.5 més endavant.

A continuació s'exposen els detalls en relació a les Fases de l'execució del contracte, el servei d'explotació que inclou, allotjament, explotació d'aplicació i serveis addicionals; i evolutius.

6.4.2 Fases de l'execució del contracte

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

<table>
<tr><td colspan="4">2025</td><td rowspan="2">2026</td><td rowspan="2">2027</td><td rowspan="2">2028</td><td rowspan="2">2029</td></tr>
<tr><td>T1</td><td>T2</td><td>T3</td><td>T4</td></tr>
<tr><td>Fase de transició de l'operació del Servei</td><td></td><td></td><td></td><td></td><td></td><td></td><td></td></tr>
<tr><td></td><td colspan="7">Fase de prestació del Servei</td></tr>
<tr><td></td><td></td><td></td><td></td><td colspan="4">Fase d'Adeqüació del Servei</td></tr>
<tr><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td>Fase de devolució del Servei</td></tr>
</table>

1) Transició de l'operació del servei: des de l'adjudicació del contracte i, com a màxim, fins a la finalització del 1er trimestre de 2025. Aquesta fase es descriu en detall en el punt "6.8 - Transició de l'operació del servei actual" del present document.

2) Prestació del servei de certificació: des de principis del mes de abril de 2025 i fins a la finalització del contracte. Com a punts clau a tenir en compte en aquest període, cal esmentar:

a) L'auditoria biennal EIDAS vigent a la celebració d'aquest contracte va tenir lloc en data 28 de març de 2013. Per tant, la primera auditoria EIDAS completa en l'àmbit temporal d'aquest contracte ha de tenir lloc en data 28 de març de 2025.
b) Sens perjudici del que s'esmenta en el punt anterior, Mozilla requereix l'enviament d'auditories anuals de revisió dels serveis. En aquest context, el Consorci AOC haurà de passar una auditoria que cobreixi el període entre el 28 de març de 2024 i 28 de març de 2025. Si s'escau, aquesta auditoria s'haurà de obtenir en paral·lel a la de preparació per l'inici d'emissions del traspàs del servei que es descriu al punt "6.8 - Transició de l'operació del servei actual"

3) Adequació del servei: des de l'1 de gener de 2026 fins a la finalització del contracte, 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 convenients 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.

4) 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 "6.7 Devolució del servei" 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.

6.4.3 Explotació de la Jerarquia Pública de Certificació Digital de Catalunya

6.4.3.1 Operació de la Jerarquia de Certificació

L'adjudicatari haurà d'allotjar i operar les Entitats de Certificació arrel i subordinades (en endavant, ECs), la titularitat de les quals és del Consorci AOC, com a Prestador de Serveis de Certificació per als ens del Sector Públic de Catalunya.

L'adjudicatari queda obligat a l'adequació i la plena conformitat dels serveis de la Jerarquia Pública de Serveis de Certificació Digital de Catalunya al Reglament del Parlament Europeu i del Consell relatiu a la identificació electrònica i als serveis de confiança per a les transaccions electròniques en el mercat interior (en endavant, "ReIDAS"), i a les normes tècniques que s'aprovin per a la seva aplicació. En aquest sentit, el contractista haurà d'obtenir a la seva costa i en els terminis establerts en la normativa aplicable, l'avaluació periòdica de la conformitat i complir amb la resta d'obligacions del Consorci AOC com a 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.

L'adjudicatari haurà de dur a terme les necessàries accions de comunicació i difusió de les claus i certificats de les EC's del Consorci AOC als usuaris del servei i a terceres parts.

L'adjudicatari haurà de donar suport per a les qüestions relacionades amb les ECs del Consorci AOC als supervisors que siguin convenients a cada moment:

- Ministerio de Industria, Comercio y Turismo, com a supervisor EIDAS a Espanya.
- Principals fabricants de programari d'ús generalitzat: Google, Microsoft, Mozilla, Apple, Adobe, Java, etc.

L'adjudicatari haurà de mantenir els actuals reconeixements dels certificats emesos per aquestes ECs mentre hi hagi certificats vigents.

L'adjudicatari s'haurà de sotmetre a les auditories de compliment que facilitin el reconeixement dels certificats emesos per aquestes ECs; incloent les auditories ETSI.

En relació al desplegament de la nova jerarquia de certificació de tercera generació, l'adjudicatari haurà de continuar desplegant-la fins a tancar la de segona generació, abans de la data màxima d'emissió permesa per la vigència de la subCA.

Més enllà del cessament de les activitats d'emissió de les Ecs del Consorci AOC, durant la vigència del contracte, l'adjudicatari haurà de continuar prestant els serveis per a la gestió del cicle de vida dels certificats: suspensió, activació, revocació, publicació de la informació de revocació, etc., d'acord amb el que s'estableix a la Declaració de Pràctiques de Certificació del Consorci AOC.

6.4.3.2 Prestació dels Serveis del Catàleg de Certificats del Consorci AOC

Independentment de la jerarquia de certificació (ECs) utilitzada per l'emissió en cada moment del contracte, l'adjudicatari haurà d'ajustar a la normativa vigent el catàleg de perfils de certificats del Catàleg de Certificats del Consorci AOC en el moment de l'adjudicació.

El catàleg de certificats de l'SCD es podrà modificar durant la vigència del contracte, per adequar-lo als canvis normatius que es produeixin; o per atendre demandes específiques dels usuaris del servei. El primer cas no generarà costos emergents per al Consorci AOC; en el segon cas, la creació de fins a dos (2) perfils nous per any no generarà costos emergents per al Consorci AOC sinó que aquests estaran inclosos en l'import fix del servei. En el cas d'eliminació d'algun perfil, l'adjudicatari estarà obligat a mantenir el suport als certificats emesos amb el perfil en qüestió durant la vigència del contracte i fins a l'extinció de la vigència de tots els certificats del mateix perfil.

Per garantir l'alineació dels certificats a emetre amb els requeriments de la legislació d'administració electrònica, el contractista ha de mantenir, a la seva proposta, la diferenciació entre certificats de classe 1 i de classe 2 o de persona vinculada. Els certificats de classe 1 correspondran, com a mínim, amb els certificats de segell electrònic i d'empleat públic, mentre que la resta de certificats podran ser també de classe 2. Aquesta restricció es podrà eliminar en funció de les condicions d'implementació del nou Reglament europeu, per a la qual cosa el contractista haurà de fer una proposta, un cop adequat a la nova regulació, i rebre la conformitat prèvia del Consorci AOC.

L'adjudicatari haurà de gestionar els necessaris reconeixements dels perfils de certificats que conformin el catàleg del Servei de Certificació Digital (SCD) del Consorci AOC als principals navegadors, fabricants de programari i validadors.

6.4.3.3 Aplicació PKI

Caldrà que l'aplicació de gestió de la infraestructura de clau pública (PKI) aportada estigui certificada Common Criteria EAL 4+.

D'aquesta manera es s'assegura que la solució aportada minimitzi els riscos derivats de les necessitats d'integració de la solució PKI aportada per l'adjudicatari amb el programari de l'entitat de Registre T-CAT i idCAT i les aplicacions i connectors desplegats a l'actual sistema de l'SCD; per tant, que minimitzi els principals riscos del projecte relatius a la gestió del canvi dels usuaris del servei.

Es requereix que l'aplicació de gestió de certificats estigui configurada per aproximar-se tant com sigui possible a la política de seguretat CIMC (Certificate Issuing and Management Components Protection Profile).

Les credencials d'accés a qualsevol part o transacció de l'aplicació seran sempre amb targeta criptogràfica i assignada nominalment a un titular (Model basat en CWA 14167).

La solució d'infraestructura de clau pública (PKI) aportada per l'adjudicatari haurà de permetre la devolució del servei a la finalització del contracte, per si en un futur es requereix transferir el servei a un nou gestor.

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 i configuracions del programari de la PKI emprat per a l'operació de les ECs que conformen la jerarquia de certificació del Consorci AOC.

El punt "6.4.2 - Fases de l'execució del contracte", estableix la data a partir de la qual tota la gestió del servei s'haurà de realitzar amb la solució PKI aportada per l'adjudicatari.

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 actuals segons s'ha definit a "6.3.3.2.1 Emissió de Llistes de Revocació de Certificats (CRL's)" i "6.3.3.2.2 Servei de Consulta d'Estat de Certificats en Línia (OCSP)".

6.4.3.4 Infraestructura tecnològica

6.4.3.4.1 Entorns

Per tal de complir amb els requisits de continuïtat dels serveis definits al pla de continuïtat del Consorci AOC que s'exposen al punt "6.4.11 La gestió de la continuïtat i la disponibilitat" d'acord als ANS definits a l'apartat "6.5.2.2 ANS de continuïtat", l'adjudicatari haurà de desplegar la infraestructura en els següents entorns:

6.4.3.4.1.1 Producció :

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.

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

6.4.3.4.1.2 Contingència:

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. També per l'entitat de certificació arrel.

6.4.3.4.1.3 Preproducció:

Desplegament d'un entorn estable complet, destinat a la formació, 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.

6.4.3.4.1.4 Entorn de proves/formació :

Desplegament d'un entorn estable complet destinat a la formació i amb la mateixa versió d'aplicació desplegada que a Producció. Tota la seva activitat no tindrà impacte en el conjunt de dades reals ni afectarà al rendiment dels altres entorns.

6.4.3.4.1.5 Desenvolupament:

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.

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.

6.4.3.4.2 CPD's

Donat que els custodis de les targetes d'administració (ACS) dels dispositius criptogràfics (HSM's) en els què s'allotjaran les claus de les EC's del Consorci AOC serà personal vinculat al mateix Consorci AOC, i amb l'objectiu de minimitzar els desplaçaments que aquests hagin de fer cada vegada que calgui realitzar una intervenció sobre aquests dispositius que requereixi que els custodis es personin per aportar i fer ús de les targetes en qüestió; es requereix que el CPD principal (CPD-1) estigui ubicat a l'àrea metropolitana de Barcelona.

La infraestructura tècnica dins del CPD principal ha de ser exclusiva de l'adjudicatari, i ha de trobar-se en una cambra amb condicions de seguretat i nivell de protecció contra qualsevol agressió física que pugui afectar els equips informàtics o de telecomunicacions i haurà de ser conforme als requisits que, sobre aquest aspecte, imposen les normes tècniques aplicables als prestadors de serveis de confiança que emeten certificats qualificats; com ara, l'ETSI EN 319 411-2 i altres més específiques que el licitador pot indicar si en disposa.

El CPD de contingència (CPD-2), 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. També per l'entitat de certificació arrel. 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).

6.4.3.4.3 Maquinari i programari dedicat

Les claus de les EC's del Consorci AOC s'hauran de generar i mantenir dins de dispositius criptogràfics (HSM) d'ús exclusiu per al Consorci AOC. També la l'aplicació PKI de gestió de certificats, ha de ser per ús dedicat a les EC's del Consorci AOC. La configuració serà en alta disponibilitat per l'entorn de Producció de les EC en línia (o EC subordinades) i, si la capacitat ho permet, també per contingència. Pel que fa als entorns de la EC arrel, el servei s'oferirà amb un dispositiu per cada entorn (producció i contingència).

El Consorci AOC preveu un escenari en el què l'adjudicatari pugui reutilitzar els HSM actuals que donen servei a les EC's subordinades. El maquinari que es posarà a disposició es recull en l'annex "Annex_11_Actius SCD-AOC.pdf"

Al llarg de la vigència del present contracte, s'ha previst (en l'import a tant alçat) que anualment l'adjudicatari adquireixi i renovi aquests dispositius, juntament amb els eventuals 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.

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 correcte 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.

6.4.3.4.4 Ús d'actius del Consorci AOC

El document annex "Annex_11_Actius SCD-AOC.pdf" del plec de prescripcions tècniques, mostra la relació d'actius que donen suport als serveis de certificació de la jerarquia actual i a l'aplicació de registre.

El Consorci AOC cedirà a l'adjudicatari l'ús del maquinari que es relaciona en aquest document a l'apartat Maquinari dedicat; i també els dispositius criptogràfics actuals. El maquinari virtualitzat es cedirà en suport digital. La cessió del maquinari compartit físic es pot negociar amb l'adjudicatari, si és del seu interès. Les prestacions i volums del maquinari com a servei i l'emmagatzematge necessari s'indiquen com a referència.

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 "6.3.3". També les fitxes d'alta dels ENS i ER amb la seva informació verificada i els operadors i rols que les composen.

En cas de donar de baixa els actius cedits, l'adjudicatari ho haurà de notificar al Consorci AOC, per tal que aquest pugui actualitzar convenientment el seu inventari d'actius.

6.4.4 Explotació del programari de l'Entitat de registre T-CAT

L'adjudicatari haurà d'allotjar, operar i mantenir el programari de l'Entitat de registre T-CAT propietat del Consorci AOC.

La línia mestre del model de registre T-CAT té l'objectiu d'equilibrar la proximitat amb els subscriptors, per mantenir un nivell alt del servei, i la racionalització del mateix, per ajustar la despesa al mínim necessari.

El nivell de servei desitjat quedaria definit pels següents atributs:

- Rapidesa en el procés de registre i proximitat amb els usuaris subscriptors.
- Mantenir la capacitat de personalització de les EERR distribuïdes pel territori sense sacrificar en excés la usabilitat i la facilitat del procés actual.
- Mantenir l'actual nivell de digitalització i seguretat del procés de sol·licitud, emissió i lliurament de certificats actual.

Els objectius d'aquesta premissa no són altres que:

- Complir ANS per al lliurament de les targetes, distingint entre el servei estàndard, el personalitzat i el servei avançat.
- Consolidar un model econòmicament auto-suficient, amb una política de preus públics de constitució i manteniment, que permetin finançar l'estructura necessària per al nou model de Registre.
- Consolidar un model de procés de servei de certificació digital a ciutadans i treballadors públics independent de la tecnologia de certificació amb alts nivells de digitalització, seguretat i usabilitat.

Tal i com s'ha exposat en els punts anteriors, el Servei de Certificació Digital T-CAT es composa de tres elements principals:

- Aplicació ASCD d'EACAT: per fer la tramitació de sol·licitud i modificació de rols en el servei de forma digital, segura i amb mecanismes per fer el seguiment del tràmit.
- Web d'Operadors de l'Entitat de registre: per a les operacions de registre de dades de subscriptors, emissió de targetes, documentació i gestió del cicle de vida del certificat digital per mitjans web i també mitjançant connectors automàtics.
- Carpeta del subscriptor: per fer el lliurament dels certificats T-CAT de forma segura i enviant els codis d'activació per correu electrònic.

El Consorci AOC valora molt el model actual de prestació del servei i el nivell de digitalització aconseguit en el procés de l'SCD T-CAT actual. Per això demana mantenir funcionalitats claus en aquest procés per garantir la persistència d'aquest model. Al mateix temps, vol minimitzar l'impacte en els usuaris operadors de l'SCD actual sense perdre de vista l'objectiu de racionalització. Per tot això, es demana que:

Amb l'objectiu de mantenir l'EACAT com a mecanisme d'entrada de les tramitacions relatives a l'SCD T-CAT i per l'elevat volum d'usuaris que utilitzen aquesta aplicació, es requereix que l'adjudicatari mantingui totes i cadascuna de les funcionalitats a alt nivell i propòsit d'aquesta aplicació ASCD dins l'SCD T-CAT.

Per dur-ho a terme, el Consorci AOC requereix a l'adjudicatari de fer una nova aplicació fora d'EACAT que compleixi les funcionalitats que cobreix actualment l'ASCD. El Consorci AOC lliurarà un prototip "cloud-native" operatiu per tal que l'adjudicatari el pugui acabar de desenvolupar, allotjar i integrar amb el nou EACAT 3.0. Aquest prototip ha estat desenvolupat a partir de les històries funcionals existents i amb millores de l'experiència d'usuari d'acord amb les indicacions del Consorci AOC.

Amb l'objectiu de facilitar el manteniment a l'adjudicatari i generar-li estalvis, el Consorci AOC preveu que l'adjudicatari pugui canviar la capa del web d'operadors actual de l'SCD T-CAT per a la seva tecnologia d'entitat de registre. Els requisits funcionals d'aquesta nova capa a proveir es detallaran en propers punts.

Pel que fa a la Carpeta del subscriptor, també es demana a l'adjudicatari que mantingui la funcionalitat d'aquest component del procés de l'SCD.

L'aplicació ASCD i la Carpeta del Subscriptor han nascut en sistemes diferents i heterogenis. L'adjudicatari pot proposar d'unificar aquestes capes de serveis de valor afegit en un sol

programari de registre que unifiqui els sistemes i que serà retornat al Consorci AOC en la fase de retorn del servei. Per dur a terme aquesta transformació, es permet a l'adjudicatari que la pugui executar durant la fase de transformació i optimització i no cal que ho faci durant la de transició. Els desenvolupaments fets en aquesta capa de valor afegit han d'anar enfocats a l'objectiu de garantir el retorn del servei al Consorci AOC de tal manera que futures transicions de tecnologies de certificació no impactin en l'experiència d'usuari dels subscriptors de l'SCD.

Pel que fa als rols enumerats en el punt “6.3.4.2 Rols del sistema T-CAT” sobre aquesta part de l'aplicació (ASCD i Carpeta del Subscriptor), es demana que l'adjudicatari els mantingui per tal d'aprofitar la tasca de creació de rols que porta fent el Consorci AOC des de fa temps i per minimitzar l'impacte en els usuaris actuals.

6.4.4.1 Entitat de registre T-CAT

Tal i com ja s'ha dit en punts anteriors, l'adjudicatari podrà canviar la capa de Registre actual per la que ell disposi. Aquesta capa de programari es situa, en termes de passos en el procés d’emissió, entre l'ASCD i la Carpeta del subscriptor. Els requisits que posa el Consorci AOC per a aquesta transformació són que la capa d'ER sigui capaç de:

Substituir les responsabilitats del mòdul peticionari actual per mecanismes d'entrada via web i automàtics per a la càrrega de dades de sol·licituds per a la seva validació i generació.

Disposar d'una interfície web i automàtica per fer la validació de dades d'una sol·licitud (actual mòdul aprovador). Les sol·licituds que vinguin per EACAT vindran ja pre-validades i, per tant, aquest mòdul i rol pot ser simplificat per a aquests casos.

Disposar d'un mòdul de generació de certificats. Aquest mòdul es correspon amb l'actual mòdul generador. Ha de suportar la generació de certificats en targeta de forma personalitzada i també de la resta de certificats del catàleg de serveis sol·licitat. La funcionalitat de generació de targetes i de la seva personalització es descriu en els propers apartats específics.

Aquest mòdul de generació de certificats pot suportar, a decisió de l'adjudicatari i només per a algunes ER concretes, un mecanisme d'emissió per lots enviats al fabricant. O alternativament, per fer una aplicació a banda amb aquest propòsit. En tot cas, l'adjudicatari haurà de contemplar aquest servei i podria aprofitar l'actual esquema de missatgeria per a l'intercanvi de dades per fer aquesta personalització de lots de targetes al fabricant.

Disposar d'un mòdul de gestió d'estats dels certificats. Aquest mòdul ha de poder ser utilitzat via web o bé via connector automàtic. Es correspon amb l'actual mòdul de gestor de certificats.

Tenir connectors de consulta d'estat de certificats per donar resposta a les necessitats dels connectors actuals. En concret, les consultes poden ser sobre un certificat en particular o múltiples certificats (els associats a una ER, per exemple, que es puguin demanar a mode d'informe) i es poden sol·licitar consumir de forma síncrona o asíncrona (cas dels informes diaris).

6.4.4.1.1 Mòdul generador: el servei de personalització de targetes a les ER's col·laboradores

Partint de l'escenari de dissenys que es descriu al punt “6.3.4.3.6 Models de provisió dels suports criptogràfics”, l'adjudicatari haurà d'ajustar el servei de creació de noves ER per a la personalització de targetes a aquests models de prestació del servei:

6.4.4.1.1.1 ER T-CAT estàndard:

ER amb impressora de plàstics (no criptogràfica) que grava certificats a una targeta amb disseny estàndard T-CAT definit pel consorci AOC. Aquest tipus d'ER és el que donarà continuïtat, en el nou model de prestació del servei, a les ER T-CAT amb targeta estàndard actual.

La targeta T-CAT estàndard que s'utilitzarà en aquestes ER serà proveïda per l'adjudicatari a l'ER sota una sèrie de condicionats que es defineixen en propers punts.

En cas que l'ER tingui impressora, la impressió de la targeta en aquestes ER serà només per la cara del davant i sense cap altra personalització ni foto. La impressora que realitza aquesta impressió, per tant, pot no tenir lector/gravador de xips criptogràfics.

No serà responsabilitat de l'adjudicatari la provisió de la impressora. No obstant, sí que se li demanaran serveis relacionats amb l'homologació, el manteniment i la formació relacionats amb les impressores de targetes.

El procés de gravació del xip i el procés d'impressió poden fer-se en un mateix pas o fins a un màxim de dos passos, de cara a mantenir la usabilitat i la facilitat del sistema actual on es fa en un sol pas.

L'aplicació d'impressió de la targeta serà desenvolupada i mantinguda per l'adjudicatari. Per tal que aquesta aplicació funcioni correctament d'acord amb el nivell de servei acordat, l'adjudicatari mantindrà un llistat de programari i impressores homologades per funcionar amb la seva aplicació i sistemes operatius usuals a cada moment de la prestació del servei. Els serveis d'instal·lació i validació de l'aplicació de personalització de targetes per a la posada en marxa de l'ER seran oferts per l'adjudicatari. No es preveu que l'adjudicatari proveeixi el maquinari (PC) per allotjar aquestes aplicacions locals de gravació i personalització en les entitats de registre.

Es pretén que les aplicacions de gravació de xip i personalització funcionin amb equips (PC) estàndard proveïts pels propis Ens que són o seran Entitats de Registre. L'objectiu d'aquest fet és no haver d'oferir manteniment a nivell de maquinari a aquests equips PC o lectors associats a l'ER.

Tot i no haver de proveir el maquinari PC, sí que l'adjudicatari haurà de mantenir una configuració homologada de sistema operatiu i components de maquinari per a l'ús d'aquestes aplicacions per garantir-ne la operativitat i l'acord de nivell de servei aplicable a l'ER. Aquesta configuració es passarà als ens que vulguin establir-se com a ER per tal que puguin adquirir el maquinari necessari. L’aplicació de generació de targetes mantindrà la funcionalitat de generar el certificat dins el xip i canviar els codis de pin i puk de la targeta. També s'integrarà amb la Carpeta del subscriptor per guardar el pin i puk generats en el moment de la generació del certificat dins el xip. També carregarà a la carpeta del subscriptor el document amb el contracte per al lliurament del certificat i altres dades addicionals que puguin caldre.

En un mateix Ens hi pot haver més d'un punt de registre. Tot i que, en la mesura del possible, la replicació de la instal·lació serà duta a terme pels propis Ens, l'adjudicatari donarà suport a la replicació. Tampoc s'aplicaran costos per llicenciament addicional del programari de l'estació de registre en aquest context, si s'escau.

L'aplicació de generació deixarà traces en el sistema que facilitin el diagnòstic de incidències puntuals de generació. També disposarà d'un conjunt d'scripts per fer tests unitaris de cada component que composa l'estació (lector extern, impressió, etc..) per tal de facilitar el diagnòstic d'incidències al CAU remot.

6.4.4.1.1.2 ER T-CAT personalitzada sense característiques avançades

ER amb impressora de plàstics (no criptogràfica) que no utilitza la targeta estàndard del Consorci AOC. Apart de requerir el nivell de servei i funcionalitats d'una ER estàndard, pot requerir un nivell de prestació de servei més elevat degut al nivell de personalitzacions que requereix la targeta que s'hi genera.

Aquestes ER pacten els seus dissenys amb els fabricants i poden requerir uns mapes i nivells de personalització més elevats.

Les personalitzacions suportades pel model personalitzat i que se surten del model estàndard poden ser únicament la foto del subscriptor i la impressió de dades (de dins o de fora del procés de registre del certificat) per la part de davant o de darrera.

També es poden emetre certificats directament a la targeta sense necessitat d'impressió, en aquests casos.

6.4.4.1.2 Principis generals del model de provisió de targetes i maquinari per a les ER T-CAT i el servei de manteniment associat a aquestes

La impressora de targetes no està inclosa en el servei de creació d'ER T-CAT que se sol·licita i serà sempre proveïda per l'ens que es vulgui constituir com a ER en base als requisits que li faciliti l'adjudicatari. Els fungibles d'aquesta impressora tampoc els proveirà l'adjudicatari.

Els licitadors oferiran com a servei l'adquisició de targetes T-CAT estàndard o altres models concrets. Aquest servei inclourà la provisió del plàstic, l'enviament a l'ER i la gestió de l'estoc. Aquesta gestió es farà des de l'ER ubicada a les instal·lacions de l'adjudicatari.

La papereria i material divulgatiu serà adquirit per l'adjudicatari per a la seva distribució a les ER estàndard i per a l'ús en la pròpia ER de les seves oficines.

L'adjudicatari es farà càrrec del manteniment i la transició de les ER actuals obertes al nou model durant la fase de transició. Per fer-ho, s'acordarà amb el Consorci AOC l'assignació de les noves tipologies d'ER a cadascuna (estàndard o personalitzada).

6.4.4.1.3 ER vinculades

D'acord amb el que s'ha exposat fins ara, les ER vinculades han de seguir sense tenir necessitat de disposar de maquinari específic per seguir fent la seva funció i rols dins de l'SCD i de seguir utilitzant les mateixes interfícies o molt similars. L'objectiu que no calgui fer formació als operadors d'aquestes ER o que, en tot cas, sigui mínima, és fonamental per garantir la continuïtat del model de registre T-CAT.

6.4.4.1.4 Interfícies i connectors

L'adjudicatari haurà de mantenir totes les interfícies actuals que hi ha interconnectades amb clients i que estan definides en el punt “6.3.4.4 Descripció de components i interfícies de programari del Servei de Certificació Digital (T-CAT i idCAT)” d'aquest document.

En particular, són especialment crítiques les que són utilitzades per clients i sistemes externs a l'SCD i, per aquests casos, caldrà mantenir exactament la mateixa funcionalitat i operativa actuals així com les mesures de seguretat pertinents i aplicables.

De forma pactada amb cada client de l'SCD i de cada connector, es podrà migrar el servei que s'ofereix actualment a alguna nova modalitat transformada.

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

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

6.4.4.2.1 EERR Virtuals / vinculades

En l'entorn T-CAT les ER's 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 a través de la carpeta del subscriptor.

El número d'ER's Virtuals o vinculades (ens donats d'alta al sistema) actualment és de 2.200.

6.4.4.2.2 ER's T-CAT

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

El número de ER's T-CAT és de 68 entitats de registre (de les quals n'hi ha que tenen varis punts d'atenció, etc...).

Les ER's T-CAT es classifiquen en dos tipologies segons el nivell de funcionalitats i personalitzacions incorporades a la targeta:

- ER estàndard T-CAT: Entitat de registre amb o sense impressora que emet els certificats T-CAT en suport targeta. El tipus de targeta és l'estàndard T-CAT que permet personalització de la part de davant de la targeta amb dades del certificat (típicament nom, organització i departament al que està adscrit el titular de la T-CAT, tot i que hi pot haver variants dels camps impresos).

- ER amb targeta personalitzada: ER amb o sense impressora que emet certificats T-CAT personals en suport targeta, però amb una targeta diferent de la T-CAT estàndard. En cas que imprimeixi la targeta, ho pot fer amb un mapa de camps personalitzat per la part de davant o de darrera de la targeta i pot incloure foto.

La informació relativa a les personalitzacions i funcions que incorpora cada ER a les targetes que emet es recull en el document "Annex_9_Resum_caracteristiques_ERs_TCAT". Aquest mateix document també conté informació relativa a les necessitats de les diferents ERs.

6.4.4.3 Servei d'emissió de suports criptogràfics

Els models de xips criptogràfics suportats i homologats actualment per a l'emissió de certificats són:

- Sm@rt cafe 7.0 del fabricant G&D
- CHIPDOC V2 ON JCOP 3 P60 in SSCD configuration, version V7b4_2

El model “Sm@rt cafe 7.0 del fabricant G&D” però, ja no s’usa per emetre certificats qualificats perquè va sortir de la llista de qualificats el juliol de 2023.

Durant la vigència del contracte es preveu que caldrà homologar almenys una nova targeta per la caducitat del dispositiu criptogràfic.

6.4.5 Model de registre idCAT certificat

L’idCAT ofereix diferents mecanismes d’autenticació i signatura. És objecte d’aquest contracte el model de servei d'idCAT en modalitat certificat en programari (format PKCS#12). En concret, els processos de registre d’identitat, validació presencial per part d’operadors del servei i lliurament del certificat al titular del certificat digital en format pkcs#12. També són objecte d’aquest contracte, les integracions del procés de registre amb el servei de vídeo-identificació i amb el servei de custòdia de certificats remots ofert pel Consorci AOC. No és objecte d’aquest contracte la provisió de la tecnologia i serveis per la vídeo-identificació dels titulars de certificats idcat ni dels serveis de custòdia dels certificats remots. El Consorci AOC ofereix aquests serveis a través del contractes “AOC 2020 71” i “AOC-2024-17”, respectivament.

El Consorci està desplegant el registre d’usuaris basat en vídeo-identificació de forma integrada i alternativa amb el procés de sol·licitud prèvia a la validació presencial de l’identitat. Aquest servei es troba en procés de construcció prèvia a l’acreditació per part del supervisor EIDAS. L’adjudicatari del present contracte haurà de mantenir la integració per poder cridar al servei de vídeo-identificació i recuperar les dades de la validació d’identitat per continuar amb el procés de lliurament.

Es demana també, en l’àmbit del servei aplicable a l’abast d’aquest contracte, la implementació de les propostes de maquetació del conjunt de webs en l’abast del servei IdCAT que faci el Consorci AOC a l’adjudicatari. Les propostes de canvi arribaran validades pels responsables d’Accessibiltat i Experiència d’Usuari del Consorci AOC. Els canvis en aquesta part de l'aplicació es consensuaran amb el Consorci AOC al llarg de totes les fases de prestació del Servei.

En relació amb el punt anterior, actualment el Consorci AOC també està en procés de canviar la pàgina web principal del servei idCAT, sota el domini de www.idcat.cat, per presentar les modalitats del servei idCAT. Aquest web s’allotjarà en sistemes del Consorci AOC i redirigirà als usuaris que desitgin un idCAT en modalitat certificat als que allotgi l’adjudicatari del present contracte.

En relació a la part del web d'operadors, el Consorci AOC demanarà a l’adjudicatari de canviar la web d'operadors actual per una versió en estat de prototip funcional, desenvolupada amb tecnologies basades en micro-serveis i que ha estat validada a nivell d’experiència d’usuari. El requisit fonamental serà que es segueixi mantenint el grau actual de separació tecnològica entre el component de Registre i el component d'Entitat de Certificació. L'adjudicatari ha de vetllar perquè aquest model es mantingui en la solució que proposi. També que l'impacte en l'alt volum d'operadors actualment formats sigui el mínim possible arran d'aquest canvi.

Les ER idCAT no tenen requisits específics de maquinari PC ni lectors. Això ve donat pel fet que tota la interacció amb l'aplicació és web i es fa des d'un navegador. Per tant, l'adjudicatari no haurà de proveir aquest maquinari sinó que haurà de mantenir unes taules de compatibilitat i requisits de components de maquinari i programari compatibles amb el servei d'entitat de registre.
L'adjudicatari inclourà en els seus serveis, el de creació d'una entitat de registre idCAT. Els serveis en què es desglossarà aquest servei de creació seran bàsicament dos: el suport per

mitjans electrònics per a la configuració dels llocs de Registre per part del propi ens i la formació per mitjans electrònics dels operadors.

A nivell de suports d'emissió, l'idCAT ha de seguir podent emetre amb el suport actual en format programari, amb generació de claus a la CA i lliurament en format PKCS#12. També haurà de permetre la gestió de les credencials de signatura remota mitjançant la redirecció de l'usuari als sistemes d'informació de la solució de signatura remota.

Per últim, l'adjudicatari haurà de continuar les integracions iniciades amb el sistema de repositori de dades del Consorci AOC a través del servei DESA'L per tal de donar compliment a les obligacions de custòdia de dades derivades de la normativa aplicable.

En el document annex "Annex_8_llistat_ER idCAT" s'enumeren les Entitats de Registre actives a data d'elaboració d'aquest document.

6.4.6 Servei d'Entitat de Registre T-CAT del Consorci AOC

L'adjudicatari crearà una ER del tipus estàndard a les seves oficines des d'on podrà oferir els serveis que s'ofereixen actualment a l'ER del Consorci AOC definits en el punt "o

L'Entitat de Registre T-CAT del Consorci AOC".

Aquesta ER allotjarà la interconnexió amb el sistema de lots per sol·licituds massives de cara a poder-les servir dins de l'ANS establert.

Aquesta ER suportarà el servei d'emissió en suport targeta en modalitat urgent i ordinària amb els compromisos d'ANS que apliquen ara a l'ER del Consorci AOC definits a "6.5.2 ANS d'Explotació del Servei".

Des d'aquesta ER es gestionaran els estocs de targetes i papereria que s'enviaran a la resta d'ER estàndard del territori.

6.4.7 El servei de suport

Actualment el servei 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.

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. En el cas del SCD aquest 2n nivell ja l'oferirà l'empresa adjudicatària del servei de certificació digital del Consorci AOC.

3er nivell: és personal de l'empresa adjudicatària del servei de certificació digital del Consorci AOC.

Es derivaran al nivell 3 les incidències que no es puguin resoldre al nivell 2.

6.4.7.1 Àmbits d'atenció i suport a prestar pel proveïdor:

L'adjudicatari haurà d'oferir el servei de suport a:

- Operadors de les Entitats de Registre (registradors)
- Usuaris finals (ciutadans i empleats públics)
- Integradors i altre personal tècnic al servei dels ens del sector públic de Catalunya

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.

6.4.7.2 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.

6.4.7.3 Horari d'atenció

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.

6.4.8 Serveis de formació

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.

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.

6.4.9 Serveis organitzatius

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:
  - 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 juntament amb l'adjudicatari del lot1 del present contracte.
  - Informes ad-hoc relatius a la prestació ordinària del servei.
- Suport a l'operativa de les Entitats de Registre
  - Gestió de la xarxa de les ER's
  - 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.
- Gestió dels enviaments postals dels suports criptogràfics i altres materials necessaris pel funcionament ordinari de les ER's.
- Gestió d'estocs i de la contractació per a l'adquisició dels suports criptogràfics, papereria, etc.

6.4.9.1 Validació de la documentació lliurable

El Consorci AOC és el propietari de tota la documentació elaborada per l'adjudicatari referent al servei prestat per l'adjudicatari.

El Consorci AOC serà el responsable de la validació i aprovació dels documents elaborats per l'adjudicatari.

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 disposició del Consorci AOC al repositori d'informació que el Consorci AOC hagi designat a tal efecte.

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.

6.4.9.2 Gestió de l'adquisició i provisió de materials i serveis

La gestió de l'aprovisionament defineix el model de provisió dels serveis sota demanda objecte del contracte i la política d'adquisició dels materials necessaris per a la prestació del servei sota demanda dels ens subscriptors.

Els licitadors hauran de descriure a les seves ofertes la seva proposta per a la gestió de la provisió de materials, quan l'adquisició la faci l'adjudicatari (com els suports criptogràfics, papereria, fungibles de les ERs, etc); i també les propostes per a la gestió dels materials adquirits pel Consorci AOC, fora de l'abast d'aquest contracte (les impressores per a les ERs col·laboradores dels Consells Comarcals, etc).

Les ofertes dels licitadors també hauran de descriure la seva proposta de model de provisió de serveis (per a la gestió, per exemple, de les sol·licituds d'obertura de noves ER's T-CAT col·laboradores, etc).

Les propostes han de contemplar l'ús de l'eina de Suport del Consorci AOC per donar suport a aquestes gestions.

6.4.9.2.1 Gestió del catàleg de productes i serveis

El catàleg de serveis habilita i defineix la relació entre el Consorci AOC i l'adjudicatari, detallant els serveis lliurats, la seva operativa de petició, l'àmbit dels mateixos, els nivells de servei compromesos i el cost.

Els licitadors hauran d'exposar a les seves ofertes la seva proposta de procediments i, si s'escau, d'eines per definir i mantenir actualitzat el catàleg de serveis objecte d'aquest contracte.

6.4.9.3 Gestió de la facturació

Els licitadors hauran de descriure a les seves ofertes la seva proposta per la gestió de la facturació, en els següents àmbits:

6.4.9.3.1 De l'adjudicatari al Consorci AOC:

El Plec de clàusules Administratives del present contracte estableix els requeriments i les condicions sobre la facturació de l'adjudicatari cap al Consorci AOC.

6.4.9.3.2 Del Consorci AOC als ens subscriptors del Servei de Certificació Digital

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 del SCD i dels corresponents mecanismes de reporting ja fixats en aquest plec - 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 entre el Consorci AOC i l'adjudicatari per a la gestió dels abonaments.

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.

Les factures s'emetran en format electrònic sempre que sigui possible a través d'una plataforma de facturació i contindran la informació especificada pel Consorci AOC per a 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 pseudonimització. S'ha de permetre identificar la comanda i cada element de la comanda 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)

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.

6.4.9.4 Funció pressupostària

El licitador haurà de descriure a la seva oferta com preveu donar suport a la funció pressupostària, especialment en cas que calgui dur a terme accions extraordinàries per cobrir eventualitats no previstes.

L'adjudicatari elaborarà els informes pressupostaris sobre els serveis contractats, amb periodicitat inicial anual, d'acord amb el calendari que el Consorci AOC estableixi.

Els informes pressupostaris elaborats han de permetre disposar d'informació suficient per a la previsió anual general de la gestió del servei.

6.4.10 La gestió de la seguretat i el compliment normatiu

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.

6.4.10.1 Classificació de la informació

L'adjudicatari haurà de tenir en compte la classificació de la informació de les aplicacions, objecte del contracte, realitzada pel Consorci AOC, per aplicar correctament el marc normatiu i legal indicat anteriorment.

6.4.10.2 Compliment normatiu i legal

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 i GDPR – General Data Protection Regulation, eIDAS - electronic IDentification, Authentication and trust Services)).

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 determinin 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 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.

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 mínims.

6.4.10.3 Requisits de protecció de dades

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 per cadascun dels àmbits especificats en l'apartat "6.3.3 Explotació de la Jerarquia dels Serveis Públics de Certificació de Catalunya" del present PPT i per tot el cicle de vida de les dades, inclòs el seu bloqueig en compliment de l'establert a la LLOPDiGDD. 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).

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

6.4.10.4 Gestió de traces

L'adjudicatari haurà de complir amb la norma de gestió de traces vigent. L'adjudicatari haurà d'assegurar que emmagatzema totes les traces que li són d'aplicació d'acord a la seva classificació d'informació i al marc normatiu i legal aplicable definit al punt "3 MARC NORMATIU".

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.

L'adjudicatari, tenint en compte el nivell de classificació de seguretat de l'aplicació exposat al punt 6.4.10.9 Auditoria externa, 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.

Trasllat al Consorci AOC de les dades i traces generades coma molt en periodicitat anual. Com a mínim certificats emesos, llistes de revocació (CRL), signatures d'aprovació o lliurament.

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

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

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

L'adjudicatari haurà de:

- Garantir que el disseny de l'arquitectura de la solució permet assolir els requeriments de disponibilitat/continuïtat requerits.
- 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.

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

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.

6.4.10.8 Seguretat en el cloud

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. En concret, caldrà que aquests entorns estiguin inclosos en l'abast de l'auditoria d'ENS i EIDAS que dugui a terme l'adjudicatari.

6.4.10.9 Auditoria externa

L'adjudicatari haurà de disposar, a partir de l'inici de la fase de transició i fins a la finalització del contracte, de la certificació de compliment , 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 l'assoliment d'aquest requeriment:

- Esquema Nacional de Seguretat (ENS):
    - 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 SCD						
Denominació de l'actiu essencial	C	I	D	A	T	DP
Subsistema repositori de jerarquia de claus de l'entorn principal (HSMs)	A	A	A	M	M	N/A
Subsistema repositori de jerarquia de claus de l'entorn de contingència (HSMs)	A	A	A	M	M	N/A
Subsistema d'emissió i revocació de certificats de l'entorn principal (PKI + CRL + OCSP)	M	M	A	M	B	M

Subsistema d'emissió i revocació de certificats de l'entorn de contingència (PKI + CRL + OCSP)	M	M	A	M	B	M
Subsistema d'Informació pública (claus públiques i documentació jurídica)	B	B	A	M	M	NA
Subsistema de suport	B	M	M	B	B	B
Subsistema de EACAT i MUX	B	B	A	M	M	M
Valor màxim registrat	A	A	A	M	M	M
La valoració del sistema es Alta (C=A, I=A, D=A, A=M, T=M, DP=M)						

  - Els subsistemes marcats en color blau, 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.
  - RTO i RPO segons definit al punt "6.5.2.2 ANS de continuïtat".

- Accessibilitat:
  - Compliment normatiu normes accessibilitat aplicables.

- Pla de Seguretat del Consorci AOC:
  - Política de seguretat i normes derivades (veure punt "3 MARC NORMATIU").

- 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 certlint o eines equivalents

  - el Consorci AOC se sotmet amb periodicitat bi-anual a les auditories que li permeten renovar els segells EIDAS esmentats en el punt ""6.4.12 Auditories del Prestador de Serveis de Certificació Consorci AOC".

  - Auditories periòdiques de les ERs : l'adjudicatari d'aquest lot haurà d'aplicar les mesures derivades del resultat de les auditories de l'adjudicatari del lot d'auditories de les ER.

6.4.11 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.

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)

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

L'adjudicatari haurà de documentar, desenvolupar i implantar les mesures de disponibilitat necessàries per cobrir els indicadors de nivell de servei de disponibilitat que es requereixen a "6.5.2.3 ANS de disponibilitat". Aquesta documentació s'haurà de lliurar al Consorci AOC.

L'adjudicatari haurà d'implantar mesures sobre els actius implicats que li permetin elaborar i lliurar al Consorci AOC un Pla de Continuïtat del servei de Recuperació davant Desastres (en endavant, PRD) per garantir els nivells de servei establerts al punt "6.5.2.2 ANS de continuïtat" d'aquest document i que 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.

L'adjudicatari haurà de mantenir actualitzat el PRD davant canvis propis o per causes de tercers.

L'adjudicatari haurà de proveir solucions tecnològiques que permetin assolir els objectius fixats al PRD, essent aquestes certificades mitjançant proves de recuperació periòdiques.

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.

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.

6.4.12 Auditories del Prestador de Serveis de Certificació Consorci AOC

Tal com s'estableix a les obligacions essencials del contracte, l'adjudicatari queda obligat a l'adequació i plena conformitat dels serveis oferts al Consorci AOC al Reglament del Parlament Europeu i del Consell relatiu a la identificació electrònica i als serveis de confiança per a les transaccions electròniques en el mercat interior (en endavant, "ReIDAS"), i a les normes tècniques que s'aprovin per a la seva aplicació.

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.

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.

6.4.13 Servei de Manteniment Evolutiu

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 adequacions del servei. L'estimació de les dedicacions a les que es destinarà aquest servei es descriu al punt "6.4.13.5 Tasques previstes en l'àmbit del manteniment evolutiu" a continuació.

L'abast d'aquest manteniment serà el codi de l'entitat de registre (T-CAT i idCAT), amb la funcionalitat descrita als punts "6.3.4 El Servei de Certificació Digital del sector públic català (T-CAT)" i "6.3.5 El Servei de Certificació Digital per la ciutadania (idCAT certificat)" així com les dades dels perfils de certificats i les personalitzacions del producte de PKI actual descrits al punt "6.3.2 Catàleg de certificats del Consorci AOC" i "6.3.3 Explotació de la Jerarquia dels Serveis Públics de Certificació de Catalunya", respectivament. Aquesta informació es troba i custodia al gestor de codi GIT del Consorci AOC i es posarà a disposició de l'adjudicatari en fase de transició per la seva revisió, manteniment i evolució al llarg de tota la vigència del contracte.

La tipologia de canvis i adequacions a aplicar es defineixen en els sub-punts a continuació del present. La metodologia a aplicar es defineix a continuació en el punt "6.4.13.1 Metodologia". Tota la gestió d'aquests canvis i intercanvis de documents relacionats es farà a través de l'eina JIRA del consorci AOC.

Els acords de nivell de servei aplicables a les sol·licituds de Servei de manteniment evolutiu es defineixen al punt "6.5.3 ANS ".

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

- 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.

6.4.13.1 Metodologia

La proposta metodològica ha de preveure com a mínim:

6.4.13.1.1 Presa de requeriments

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

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

- Requeriments funcionals: tenen a veure amb les funcionalitats que es desitja incorporar o modificar a l'aplicació.
- Requeriments tècnics: tenen a veure amb possibles requeriments de caire tecnològic; per exemple, potser per aconseguir l'evolutiu cal utilitzar una versió determinada d'una llibreria d'un tercer. Un altre cas, pot ser que es marqui com a requeriment que una consulta en base de dades cal fer-la sobre una tecnologia determinada (potser sobre mysql).
- Requeriments de calendari: tenen a veure amb terminis de lliurament de l'evolutiu.
- Requeriments de context: tenen a veure amb la importància que pugui tenir l'evolutiu, el possible impacte sobre els clients, la prioritat de l'evolutiu respecte la resta de sol·licituds en curs i/o prèviament planificades, etc.
- Requeriments de Seguretat: incorporar tots els controls de seguretat que, pel tipus d'informació tractada, ha d'incorporar l'evolutiu

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

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'evolutiu**, amb una descripció el més detallada possible de l'evolutiu 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 vàries 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 requeriments"**, on es recullin tots els requeriments per abordar l'evolutiu, agrupats segons la tipologia descrita anteriorment.
- El Consorci AOC revisarà aquest document i es gestionaran els canvis pertinents fins la seva formalització.

6.4.13.1.2 Fase de pre-anàlisi

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

En base al "Document de requeriments", l'adjudicatari procedirà a fer un pre-anàlisi dels canvis que implicaria realitzar a l'aplicació per tal d'aconseguir l'evolutiu 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.
    - Cas que l'adjudicatari vegi vàries alternatives, explicar-les i indicar els avantatges i inconvenients de cadascuna.
- Estimació del cost en hores que implicarà l'evolutiu. 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'evolutiu..
- 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.

6.4.13.1.3 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
- Descripció de proves de validació: cal descriure les proves que es duran 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'evolutiu tenen el comportament esperat. Cal descriure totes les proves funcionals que garanteixin haver testejat totes les funcionalitats de l'evolutiu. 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'evolutiu segueixen funcionant correctament.

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

6.4.13.1.4 Fase de disseny

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

6.4.13.1.5 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.

6.4.13.1.6 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.

6.4.13.2 Manteniment correctiu

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

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.

6.4.13.3 Manteniment tècnic – legal

El servei de manteniment tècnic-legal inclourà el manteniment normatiu que actualitzi la versió de la plataforma perquè es compleixin amb els requisits legals. 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 3 sobre el MARC NORMATIU i elaborades per les organitzacions i organismes de normalització europeus, en particular pel Comitè Europeu de Normalització (CEN) i l'Institut Europeu de Normes de Telecomunicació (ETSI), així com l'Organització Internacional de Normalització (ISO) i l'Unió Internacional de Telecomunicacions (UIT).

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 fòrums 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).

6.4.13.4 Manteniment evolutiu

El servei de manteniment evolutiu, inclourà aquelles modificacions sol·licitades pel Consorci AOC, al marge de les contemplades anteriorment en els punts "6.4.13.2 Manteniment correctiu" i "6.4.13.3 Manteniment tècnic – legal".

6.4.13.5 Tasques previstes 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. En tot cas, sempre hauran de tenir encaix en les tipologies de tasques els punts "6.4.13.2 Manteniment correctiu", "6.4.13.3 Manteniment tècnic – legal" i "6.4.13.4 Manteniment evolutiu". En base als períodes anteriors i amb les noves demandes previstes en el moment de redacció d'aquest document, s'estimen aquestes tasques i dedicacions segons cada tipus de tasca en el plec de clàusules administratives.

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.

6.5 Acords de nivell de servei

El funcionament dels serveis objecte d'aquest lot 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 i Condicions de prestació específiques del Servei de Certificació Digital del Consorci AOC (publicades a https://www.aoc.cat/condicions-prestacio-serveis-aoc/).

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

- ANS d'Explotació del Servei:
  - Indicadors de compliment dels nivells de servei recollits a les Declaracions de Pràctiques de Certificació[1] 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).
  - ANS d'emissió i gestió dels certificats:

[1]Les Declaracions de Pràctiques de Certificació de les ECs del Consorci AOC es troben publicades a: https://epscd.aoc.cat/regulacio

        - Terminis de lliurament en el servei de emissió i renovació de T-CAT pels dos nivells (ordinari i urgent).
        - Observat amb eina de tiqueting/JIRA al cloud 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 ISM i splunk, o eina equivalent.

    - ANS de capacitat :
        - En transaccions per segon (tps) pels serveis web de 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.

    - 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 Continuïtat del Servei : Indicadors relatius a la gestió del pla de contingència, tal com es descriuen a "6.4.11 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 doc jurídica i FFLL, etc.)

La mesura dels ANS es farà amb eines de AOC o proveïdes per l'adjudicatari per la monitorització contínua (p.ex. eina ISM pel cas de la disponibilitat) a partir de transaccions automàtiques o interaccions humanes simulades.

Els informes de Seguiment requerits (punt 6.6) inclouran els valors d'aquests indicadors definits pel període corresponent.

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

6.5.1 Model de mesura del nivell de servei

Per tal de disposar de la informació necessària per a una gestió i governament homogeni del Servei de Certificació, 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 vàries 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 composen 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 ni-vell d'acompliment del servei aprovisionat, 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 me-sura 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.

6.5.1.1 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 referencia 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 me-sura, 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.

6.5.1.2 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 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.

6.5.1.3 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.).

6.5.2 ANS d'Explotació del Servei

Indicadors/valors de nivells de servei recollits a les Declaracions de Pràctiques de Certificació que apliquen a cada Entitat de Certificació en els següents àmbits derivats de les normes de negoci:

- Publicació d'informació i directori de certificats de les Entitats de Certificació.
- Acords de nivell de serveis relatius als procediments d'identificació i autenticació previs a l'emissió de certificats
- Compliment dels procediments relatius a l'operació del cicle de vida dels certificats.
- Revocació en cas de sospita de mal ús en 24 hores de certificat SSL.
- Emissió de la CRL de la EC arrel cada 6 mesos.
- Emissió de la resta de CRLs cada 24 h, màxim 7 dies de vigència.

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

6.5.2.1 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.

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

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.

6.5.2.2 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 AOC 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 i els Serveis de Validació (OCSP i CRL):

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

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.

6.5.2.3 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 %

  - Web operadors idCAT i T-CAT
  - Connectors de càrrega i consulta de peticions

- 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.

6.5.2.4 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 : 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.

6.5.2.5 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 pretació correcte 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 objecte d'auditoria del lot d'auditoria de les Entitats de Registre (lot 2 del present contracte).
- Per 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/awslabs/certlint) per la comparació automàtica.

6.5.2.6 ANS del Servei de Suport

L'adjudicatari, en la prestació el servei de suport de 2n i 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.

6.5.3 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 al punt "6.4.13.1" sobre la metodologia del manteniment evolutiu.

6.5.3.1 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.

6.5.3.2 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)*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.

6.5.3.3 Temps de resposta en el manteniment evolutiu

En relació al servei de manteniment evolutiu, es defineixen els següents temps a fi de fixar un Acord de Nivell de Servei:

- 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

6.5.3.4 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.

6.6 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'eficaç implantació dels controls definits.

6.6.1 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 "6.5 Acords de nivell de servei" i que apliquen als diferents àmbits del governament del servei objecte d'aquest lot. 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 format i el contingut mínim de la informació a elaborar per l'adjudicatari en tots els àmbits de governament és el definit en l'annex "Annex _1_Plantilla Informe Seguiment".

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.

6.6.1.1 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/clients 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

6.6.2 Òrgans de Gestió

6.6.2.1 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.

6.6.2.2 Reunions de Seguiment.

El gestor del servei de l'adjudicatari i el Cap del Servei del SCD 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 "6.4.10 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 el present lot.
- 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 proposat en definit en l'"Annex _1_Plantilla Informe Seguiment" que inclou, 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 lot.
- Millores aplicables al servei de certificació digital.
- 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 a 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.

6.6.2.3 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 les fases 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.

6.6.2.3.1 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 de certificació digital 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 de Certificació Digital i/o les interrelacions entres 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 "6.8 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.

6.7 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 desenvolupament realitzats pels seus serveis dins del marc d'aquest contracte (d'interfícies d'usuari i d'altres

personalitzacions). 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 PKI aportada. 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 inclou l'adquisició de les llicències necessàries pel funcionament de la solució més enllà de la finalització del contracte.

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.

Degut a la naturalesa regulada de la prestació contractual, i en els termes fixats per la legislació vigent, el contractista queda obligat, sense cost addicional, a mantenir operatius els següents serveis més enllà del termini fixat per a la prestació contractual:

- Els certificats d'autoritat de certificació i la resta de certificats d'infraestructura han de romandre vigents, sense que es pugui procedir a la seva revocació fins a l'expiració de tots els certificats d'usuaris i serveis finals que avalin – excepte per petició expressa del Consorci AOC.

- Els serveis d'informació d'estat de certificats, en forma de llista de revocació de certificats (CRL) i servei de consulta en línia de certificats (OCSP), han de romandre operatius fins a l'expiració dels certificats corresponents, i durant un període de tres mesos addicionals.

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.

6.8 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 a la PKI del Consorci AOC, de manera que, a la finalització d'aquesta fase, la prestació efectiva del servei d'emissió de certificats del Consorci AOC la dugui a terme, a tots els efectes, l'adjudicatari.

Donat que el marc normatiu aplicable regeix en tot moment, inclús durant la re-ubicació física de les dels actius del Servei de Certificació Digital a un nou CPD, el Consorci AOC, per tant, ha d'assegurar que l'accés físic als entorns segurs està limitat i autoritzat correctament, que l'equipament està operat sota el control de múltiples persones i que els accessos no autoritzats seran detectats en tot moment.

És per això que en cas que el licitador, en la seva oferta, proposi un canvi en el personal d'operació del servei o un canvi d'ubicació dels dispositius que allotgen les claus privades de

les entitats de certificació, caldrà que aporti en la seva oferta un pla de traspàs auditat per un tercer i que doni compliment a la normativa aplicable. En concret, el pla haurà de donar resposta als requisits de la Root Store Policy de Mozilla a la que està adherit el Servei de Certificació Digital del Consorci AOC (https://www.mozilla.org/en-US/about/governance/policies/security-group/certs/policy/). Concretament, en els apartats en relació a la transició de l'operació del servei actual, el que es determina, en els punts relatius al canvi de personal operador (8.2 Change in Operational Personnel) i canvi d'ubicació segura (8.3 Change in Secure Location). S'incorporen aquí els requisits més rellevants en relació a la transició de l'operació derivats de les versions vigents en el moment de la redacció d'aquest plec a mode d'exemple del compliment que caldrà evidenciar, com a mínim:

- La revisió prèvia dels actius i documentació del Servei per, si s'escau, adequar-los als canvis derivats.
- La notificació a la comunitat Mozilla del pla de canvi.
- Completar el pla de traspàs presentat a la oferta i aprovat per l'auditor corresponent.
- Aturar l'emissió de certificats a la ubicació actual abans del canvi.
- Auditar l'estat dels actius crítics (claus privades) per confirmar que estan llestos pel trasllat i per assegurar que les claus estan ben protegides a l'origen.
- La cerimònia de transferència hauria d'estar enregistrada en vídeo i disposar de la presència d'un testimoni auditor en tot moment durant l'intercanvi físic dels dispositius criptogràfics i les targetes d'administració d'aquests.
- A la nova ubicació caldrà també fer una auditoria per confirmar que la transferència ha estat satisfactòria, que la clau privada s'ha mantingut protegida durant la transferència i que les claus privades poden reprendre les emissions. Aquest requisit es pot complir amb una auditoria puntual en el temps que denoti que els sistemes estan apunt per l'emissió (PITRA – Point-in-time Readiness Audit).
- Enviament de les auditories a la comunitat Mozilla.
- En cas que hi hagi algun problema durant el canvi, informar-lo a la comunitat Mozilla també.

L'objectiu d'aquests passos és evidenciar que l'adjudicatari compleix amb els requisits derivats del marc normatiu aplicable i, en concret, amb els requisits derivats de l'esmentada política del Mozilla/CCADB .

Tal i com estableix el punt "6.4.12 Auditories del Prestador de Serveis de Certificació Consorci AOC", el cost de l'auditoria del procés de traspàs ha d'estar inclosa en els serveis que l'adjudicatari ha d'oferir en el present contracte.

El calendari i fites de seguiment específic segons estableix el punt "6.6.2.3 Model de relació en la fase de Transició de l'operació" i "6.6.2.3.1 Governament de la fase de Transició de l'operació" seran:

- Per la fase de revisió d'actius i documentació actual del Consorci AOC, el nou adjudicatari disposarà d'un termini de 3 setmanes.
- Com a molt tard als 3 mesos des de l'adjudicació, s'avaluarà si és viable iniciar les activitats de les EC's del Consorci AOC a la nova ubicació en base als resultats obtinguts en els controls tècnics i de seguretat previstos a tal efecte.

La data límit per a que l'adjudicatari inicïi l'operació dels sistemes que actualment donen suport al Servei de Certificació Digital del Consorci AOC és l'1 d'abril de 2020. Per facilitar aquesta transició, el Consorci AOC esgotarà el contracte vigent amb el proveïdor sortint. S'encoratja, per tant, a l'adjudicatari a aprofitar aquest marc contractual per assumir l'operativa i el control del servei amb el suport del proveïdor sortint.

En particular, en relació al compliment de l'Esquema Nacional de Seguretat, es requereix que l'adjudicatari hagi completat l'auditoria de compliment d'acord als termes i abast definits al

punt “6.4.10 La gestió de la seguretat i el compliment normatiu” de forma prèvia a la transició de l’operació del servei.

L'adjudicatari començarà a ingressar pels serveis sota demanda amb preu unitari, corresponents a l’emissió de certificats digitals, a partir del moment en que inicii aquesta prestació emprant la solució PKI aportada per ell.

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

7 Definicions, acrònims i enllaços d'interès

7.1 Definicions

DISPOSITIU: Suport on es graven els certificats emesos, per exemple, una targeta criptogràfica específica, un fitxer PKCS#12 en un directori, o una memòria USB. El sistema ha d'utilitzar els diferents dispositius físics via interfície PKCS#11.

ENS. Organisme amb usuaris que necessiten i utilitzen els certificats emesos.

ENTITAT DE REGISTRE. Oficina on hi ha operadors del sistema. Una Entitat de Registre pot peticionar o veure certificats d'un o varis ens sobre els que està autoritzat. Al mateix temps, pot tramitar certificats d'una o vàries Entitats de Certificació i d'un o varis perfils de certificat de cada Entitat de Certificació. Cada Entitat de certificació té un tipus especial d'Entitat de Registre (codi 000) que pot tractar certificats de qualsevol ens.

LOT. Conjunt de peticions de certificació agrupades sota un mateix identificador i que per-met realitzar operacions globals per tots els seu elements.

OPERADOR. Persona o programari, identificat mitjançant un certificat digital, que pot accedir al sistema del SCD i realitzar les funcions definides per el seus rols.

PERFIL DE CERTIFICAT. Certificat o conjunt de certificats que emet el sistema. En la definició del perfil es podran especificar coses com: certificats a emetre (per exemple firma i xifrat), dades necessàries per el certificat, dades de gestió (adreces, etc), dades per la personalització gràfica del suport (fotografia, disseny, etc.), regles d'unicitat que apliquen als certificats, etc.
En cas que un perfil generi més d'un certificat, el sistema permetrà realitzar les operacions del cicle de vida (revocació, suspensió, consulta, etc) de manera conjunta i transparent des del punt de vista dels operadors.
El sistema disposa de diferents Entitats de Certificació que al mateix temps emeten diferents perfils cadascuna. Dins el concepte perfil Cada perfil es pot generar sobre un o varis dispositius diferents.

POSSEÏDOR DE CLAUS. Usuari titular del certificat i que serà el responsable del seu ús.

RESPONSABLE DE SERVEI. És l' interlocutor i gestor principal davant del servei per un ens.

ROL. Propietat associada a un Operador i que defineix les operacions que pot fer. Un operador pot tenir més d'un rol, sempre que aquests no siguin incompatibles.

SISTEMA ONLINE. Part del sistema del SCD que permet generar certificats de manera completa a partir de les dades de la petició.

SISTEMA LOTS. Part del sistema del SCD que permet generar els fitxers a partir de l'enviament d'informació en forma de Lot al fabricant de targetes, En aquest esquema les tasques logístiques queden repartides entre el fabricant de targetes i la AOC. Aquest sistema només es aplicable a un conjunt reduït de certificats i perfils, sempre en suport targeta criptogràfica.

DOCUMENTUM. Producte comercial de gestió documental

7.2 Acrònims

ASCD. Automatització de la Sol·licitud de Certificats Digitals, mòdul de EACAT
CRL. Certificate Revocation List
CRT. Fitxer binari de certificat digital
CSR. Certificat Signing Request
EACAT. Extranet de les Administracions Públiques Catalanes
EAPC. Escola d'Administració Pública de Catalunya
EC. Entitat de Certificació
EC-ACC. Entitat de certificació Agència Catalana de Certificació
EC-AL. Entitat de certificació Administració Local
EC-GENCAT. Entitat de certificació GENCAT
EC-IDCAT. Entitat de certificació idCAT
EC-PARLAMENT. Entitat de certificació Parlament
EC-SAFP. Entitat de certificació Secretaria d'Administració i Funció Pública
EC-UR Entitat de certificació Universitats i Recerca
EC-URV. Entitat de certifiació Universitat Rovira i Virgili
eIDAS / ReIDAS. Electronic Identification and Signature (Electronic Trust Services), de la Comissió Europea
ER. Entitat de Registre
ERC. Entitat de Registre Col·laboradora
ERV. Entitat de Registre Virtual
GEDA-e. Gestor Documental intern del Consorci AOC per l'allotjament de la documentació de l'SCD
GEXAM. Gestió d'Exàmens, aplicació de l'EAPC
LDAP. Directori de dades (Lightweight Directory Access Protocol)
LRA. Local Registration Authority
MINETUR. Ministeri d'Indústria, Energia i Turisme
MUX. Servei de Registre Administratiu Unificat del Consorci AOC
OCSP. Servei de Consulta d'Estat de Certificats en línia (Online Certificate Status Protocol)
PSC. Prestador de Serveis de Certificació
SCD. Servei de Certificació Digital
SGD. Sistema de Gesió Documental
SOCEX. Servei d'Obtenció del Certificat de Xifrat. Connector del SCD del Consorci AOC
T-CAT. Nom comercial de la família de certificats personals i de dispositiu destinats al sec-tor públic català
T-CAT P. Certificat personal de treballador públic en format programari

7.3 Enllaços d'interès

Documentació Reguladora del Servei de Certificació digital del Consorci AOC : https://epscd.aoc.cat/regulacio

Portal de suport Servei T-CAT : https://suport-tcat.aoc.cat/hc/ca
Portal de suport Servei idCAT : https://suport-idcat.aoc.cat/hc/ca
Portal de suport Servei ER T-CAT : https://suport-ertcat.aoc.cat/hc/ca
Portal de suport Servei ER idCAT : https://suport-eridcat.aoc.cat/hc/ca

8 ANNEXOS

- Annex_1_ Plantilla Informe Seguiment.pdf
- Annex_2_1_ChekingAuditoria_ER_T-CAT_V6_2024.pdf
- Annex_2_2_ChekingAuditoria_ER_T-idCAT_presencial_2024.pdf
- Annex_3_AutoavaluacióEntitatsRegistre_virtual_definitiu_2024.pdf
- Annex_4_D1121 AuditoriaConformitatSCD_definitiu_2024.pdf
- Annex_5_ModelInformeAuditoriaConformitatV1_2024.pdf
- Annex_6_volumetries_emissions_2024.pdf
- Annex_7_llistat_ER_T_CAT_2024.pdf
- Annex_8_llistat_er_idcat_2024.pdf
- Annex_9_Resum_caracteristiques_ERs_TCAT.pdf
- Annex_10_Descripcio_plataforma_SCD.pdf
- Annex_11_Actius SCD-AOC.pdf
- Annex_12_ Inventari_ER.pdf

Consorci
Administració Oberta
de Catalunya

Informe de seguiment del Servei nom_sistema mes any

Generalitat de Catalunya

LOCALRET

Realitzat per: Responsable de Servei X
Versió:
Data: 09/07/2024
Arxiu: Documento1

Index

1 Seguiment de Servei

1.1 Visió general

1.1.1 Quadre de situació servei

Tipologia	Pendents inici període	En període		Pendents fi període
		Entrades	Tancades	
Incidència	14	14	16	12
Petició a mida	10	8	12	3
Petició estàndard	21	10	17	14
Total	**36**	**26**	**34**	**28**

1.1.2 Quadre d'incidències per tipologia (si n'hi ha de definides)

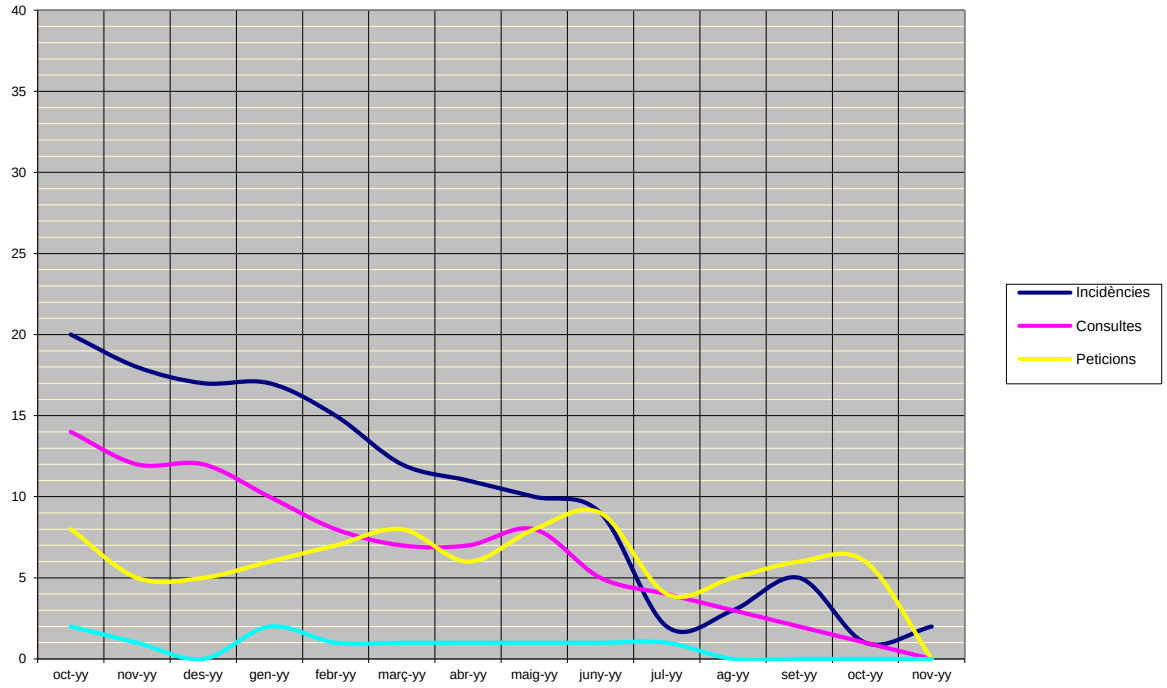
Tipologia	Pendents inici període	En període		Pendents fi període
		Entrades	Tancades	
Tipus 1	1	2	1	2
Tipus 2	14	14	16	12
Tipus 3	10	8	12	6
Total	**25**	**24**	**29**	**20**

1.1.3 Quadre d'incidències per prioritat

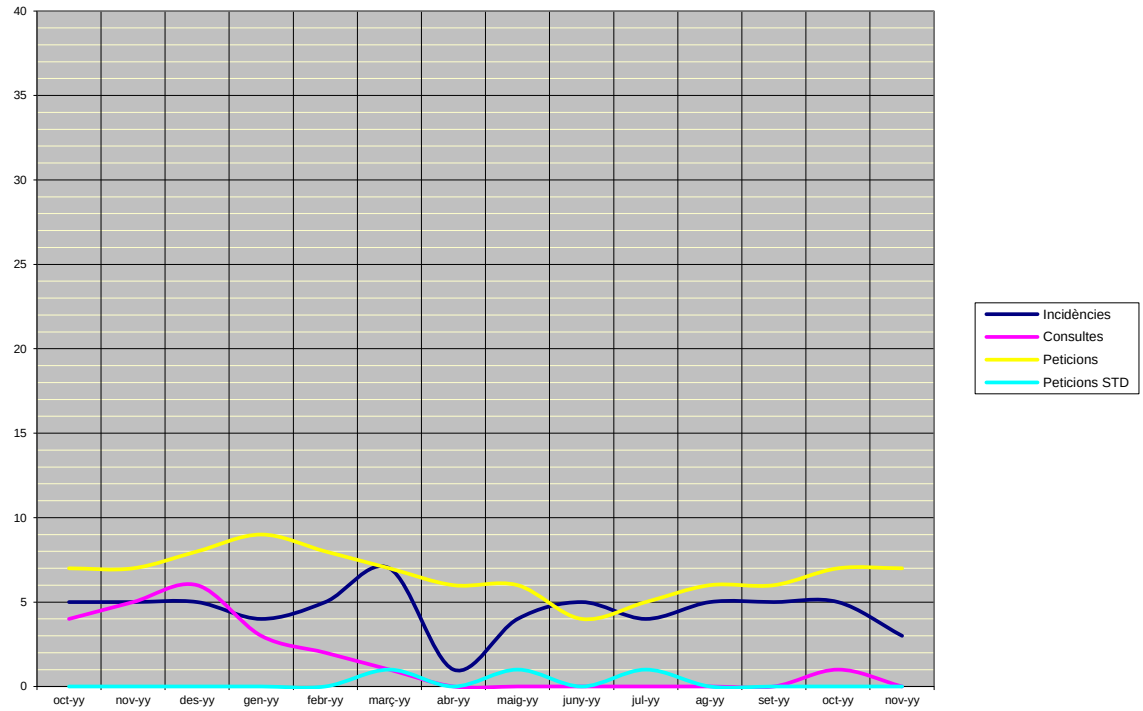
Prioritat	Pendents inici període	En període		Pendents fi període
		Entrades	Tancades	
Crítica	0	0	0	0
Alta	0	0	0	0
Important	1	2	1	2
Baixa	10	8	12	6
Total	**25**	**24**	**29**	**20**

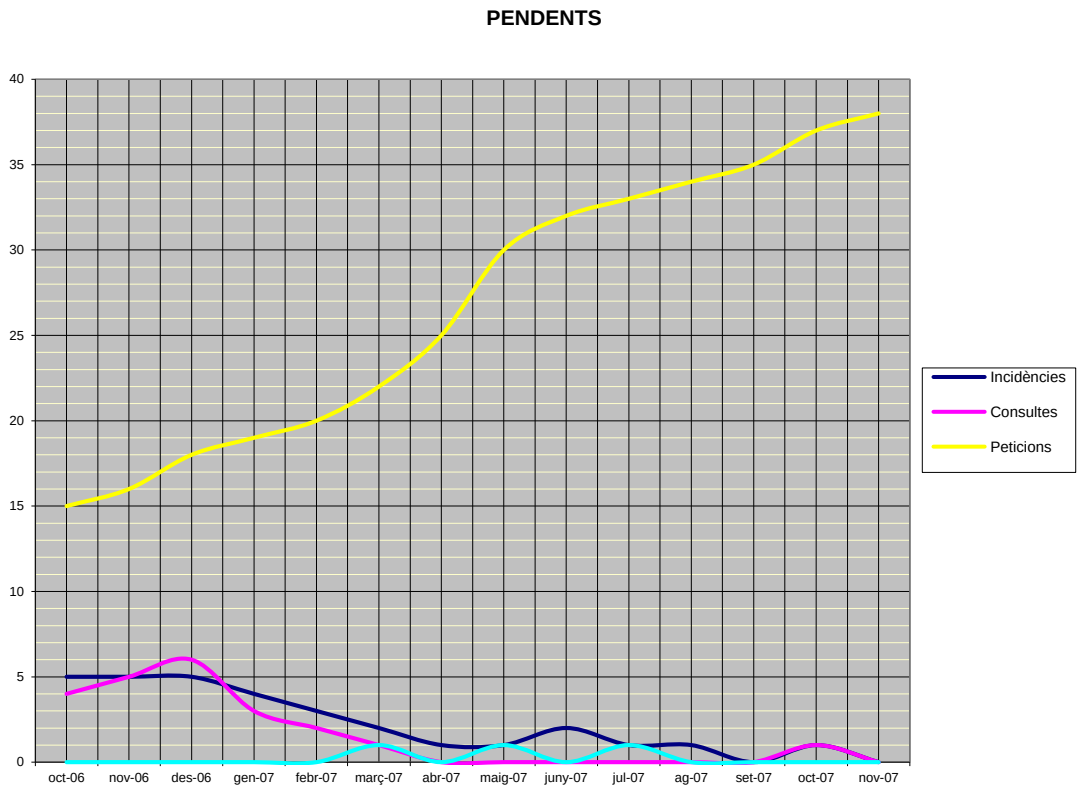
1.1.4 Gràfiques d'evolució

ENTRADES



TANCADES





1.2 Quadre de Compliment ANS

Actuacions	Acord Establert	Temps de resposta				Total
		Dins ANS'S		*Fora ANS's*		*Total*
		Nombre	*%*	*Nombre*	*%*	
Crítica	4 hores	1	100%	0	0%	1
Alta	1 dia	0	0%	0	0%	0
Mitja	4 dies	0	0%	0	0%	0
Baixa	N/A	0	0%	0	0%	0
Totals (nombre i compliment ANS)		***1***	***100%***	***0***	***0%***	***1***

1.2.1 Gràfica evolució compliment ANS

1.3 Temes tancats en el període

1.3.1 Peticions estàndard (si n'hi ha de definides)

Actuacions	Acord Establert	Temps de resposta				Total
		Dins ANS'S		*Fora ANS's*		*Total*
		Nombre	*%*	*Nombre*	*%*	
Petició 1	3 dies	4	100%	0	0%	4
Petició 2	2 dies	0	0%	2	100%	2
Petició 3	N/A	5	0%	0	0%	5
Petició 4	N/A	0	0%	0	0%	0
Petició 5	N/A	2	50%	2	50%	4
Petició 6	N/A	1	100%	0	0%	1
Petició 7	N/A	0	0%	0	0%	0
Totals (nombre i compliment ANS)		***12***	***75%***	***4***	***25%***	***16***

1.3.2 Peticions a mida

Peticions a mida tancades								
Codi	Nom	Data petició	Valoració		Data aprov.	Previsió		Data Finalització Real
			Data	Cost (*)		Inici	Final	
3874	Petició 1	10/18/17	27/02/18	1,25	09/03/18	11/04/18	27/04/18	27/04/18
1987	Petició 2	06/03/18	13/03/18	7				27/04/18

(*) Unitat de mesura (jornada/hores)

1.3.3 Incidències

Codi	Nom	Prioritat	Data obertura	Data tancament
11446	Incidència 1	Crítica	01/03/18	10/03/18
12167	Incidència 2	Crítica	01/03/18	12/03/18
18277	Incidència 3	Alta	01/03/18	15/03/18

1.4 Temes pendents a final de període

1.4.1 Peticions a mida pendents

Peticions a mida obertes									
Codi	**Nom**	**Data petició**	**Valoració**		**Data aprov.**	**Previsió**		**Estat**	**Assignada**
			Data	**Cost (*)**		**Inici**	**Final**		
6787	Petició 1	10/18/17	27/02/18	1,25	09/03/18	11/04/18	27/04/18	Escalada	Tècnic 1
18672	Petició 2	06/03/18	13/03/18	7				En Espera	Tècnic 2
19078	Petició 3	09/03/18						Escalada	Tècnic 3

(*) Unitat de mesura (jornada/hores)

1.4.2 Incidències pendents

Codi	Nom	Prioritat	Data	Estat	Assignada
11446	Incidència 1	Crítica	01/03/18	Escalada	Tècnic 1
12167	Incidència 2	Crítica	01/03/18	Escalada	Tècnic 2
18277	Incidència 3	Alta	01/03/18	En espera	Tècnic 3

Comentaris de les causes de possibles endarreriments

2 Seguiment facturació

2.1 Factures presentades.

2.2 Cost previst dels evolutius en curs.

2.3 Diners disponibles.

3 Temes a destacar del període

4 Pla d'accions

Accions			
Descripció	**Responsable**	**Data inici**	**Estat**
Petició 1	SE	15/maig/18	En curs
Petició 2	SE	6/juliol/18	En curs
Petició 3	SE	26/setembre/18	Finalitzat setembre/2018
Petició 4	PRJ	11/juliol/18	Finalitzat 29/octubre/2018
Petició 5	SE	1/octubre/2018	En curs

5 Característiques del servei

5.1 Horaris de servei

5.2 Telèfons i persones de contacte.

5.3 Descripció categories incidències

Consorci Administració Oberta de Catalunya

Dades Generals	
Entitat de Registre	
Responsable del servei	
Auditor AOC	
Data auditoria	

Informe d'auditoria d'Entitat de Registre T-CAT

Àrees	Id. Control		Control	Tipus Control	Valoració	Evidència / Observació
REQUISITS DE GESTIÓ DOCUMENTAL I ARXIU	1.1.		Tramitació dels expedients			
		1	**Metodologia d'arxiu i traçabilitat**	**OBL**	No avaluat	
		2	**El contingut dels expedients és l'adequat (Sol·licitud d'emissió, acusament de rebuda de correus i còpia del full de lliurament i acceptació de certificats signada pel titular, en els casos en que s'hagi tramitat en paper).**	**OBL**	No avaluat	
		3	**La informació dels expedients seleccionats es correspon amb la informació dels certificats emesos.**	**OBL**	No avaluat	
		4	**Els expedients estan impresos amb paper que compleix la Norma UNE-EN ISO 9706:1999.**	OPT	No avaluat	
	1.2.		Arxiu de gestió			
		1	**Els arxivadors i/o armaris de gestió romanen tancats amb clau quan el personal del servei no està present.**	**OBL**	No avaluat	
		2	**L'accés als arxivadors només es permet al personal autoritzat.**	**OBL**	No avaluat	
	1.3.		Transferència a l'arxiu central			
		1	**Existeix un procediment de transferència d'expedients que defineix la periodicitat, el responsable i el mode d'enviament físic a l'arxiu central.**	OPT	No avaluat	
	1.4.		Arxiu Central			
		1	**Els controls de seguretat física de l'arxiu són adequats.**	**OBL**	No avaluat	
		2	**Metodologia d'arxiu i traçabilitat**	**OBL**	No avaluat	

REQUISITS OPERATIUS	**2.1.**	Documentació Requerida				
	1	**Disposen d'una fitxa de subscriptor actualitzada i ha estat enviada en els darrers 2 anys**		**OBL**	No avaluat	
	2	**Disposen d'una fitxa d'entitat de registre actualitzada i ha estat enviada en els darrers 2 anys**		**OBL**	No avaluat	
	3	**Disposen de termes i condicions on hi consten:**	**Les obligacions dels subscriptors, periode de temps d'arxiu de logs, marc legal i compromis sobre disponibilitat**	**OBL**	No avaluat	
	4	**Disposen de termes i condicions on hi consten:**	**Procediment de queixes i resolució de conflictes**	**OBL**	No avaluat	
	5	**L'entitat informa prèviament als subscriptors i parts interessades sobre els termes i condicions abans d'iniciar la relació contractual**		**OBL**	No avaluat	
	6	**Els termes i condicions es troben disponibles en mitjans no peribles amb un llenguatge entenedor i es poden transmetre electrònicament.**		**OBL**	No avaluat	
	7	**Els serveis han de ser accessibles a tots els sol·licitants**		**OBL**	No avaluat	
	8	**Disposen de polítiques i procediments per a la resolució de conflictes o reclamacions de clients o altres parts interessades**		**OBL**	No avaluat	
	9	**Es diposa de la Fitxa d'identitat i s'ha revisat el compliment**		**OBL**	No avaluat	
	10	**Disposen d'un procediment de gestió d'incidents**		**OBL**	No avaluat	
	11	**Disposen d'un procediment de compliment legal i normatiu (compliance)**		**OBL**	No avaluat	
	12	**Mantenir un llistat actualitzat d'actius d'informació amb l'assignació de la classificació corresponent amb l'avaluació de riscos realitzada.**		**OBL**	No avaluat	
	13	**Es disposa d'un procediment i registre de gestió de canvis per a versions, modificacions i desplegaments.**		**OBL**	No avaluat	
	14	**Existeix un procediment de reinici i recuperació del sistema en cas que falli..**		**OBL**	No avaluat	
	15	**L'Entitat de Registre està alineada amb el pla de continuïtat de l'AOC**		**OBL**	No avaluat	
	2.2.	Formació i repàs de coneixements				
	1	**Tots els operadors han realitzat el curs formatiu d'operador d'entitat de registre T-CAT de Consorci AOC.**		**OBL**	No avaluat	
	2	**El responsable del servei mostra coneixement del procediment aprovat per tal de guardar la documentació a l'arxiu de gestió en forma d'expedient.**		**OBL**	No avaluat	
	3	**Es disposa d'una fitxa personal actualitzada amb la formació rebuda del personal involucrat.**		**OBL**	No avaluat	

	4	**Tot el personal (temporal o fixe) disposa de la seva descripció del lloc de treball on hi consta la sensibilització de posició en funció dels drets i nivell d'accés, formació i sensibilització.**	**OBL**	No avaluat	
	5	**L'Entitat de Registre té descrites sancions disciplinàries per aquells treballadors que incompleixin les polítiques o procediments establerts.**	**OBL**	No avaluat	
	6	**L'Entitat de Registre disposa de procediments i processos de gestió alineats amb els de seguretat de la informació.**	**OBL**	No avaluat	
	7	**Tots els operadors han d'estar lliures de conflictes d'interessos que puguin perjudicar la imparcialitat de les operacions del servei.**	**OBL**	No avaluat	
	8	**El personal no tindrà accés a les funcions d'operador del sistema fins que no s'hagin complert tots els controls necessaris.**	**OBL**	No avaluat	
	9	**Tots els operadors mostren coneixement del procediment per registrar i comunicar incidents de seguretat de la informació.**	**OBL**	No avaluat	
	10	**Tots els operadors han rebut una formació sobre actualitzacions sobre noves amenaces i pràctiques de seguretat actuals en els darrers 12 mesos.**	**OBL**	No avaluat	
3.1.		Seguretat física			
	1	**La sala d'operacions ha de disposar d'un sistema electrònic d'obertura o, com a mínim, d'una porta amb pany i clau. En el cas que això no fos possible, la LRA ha d'estar ubicada en un lloc reservat on només hi tingui accés el personal de l'ER i en cap cas personal aliè al Ens subscriptor.**	OPT	No avaluat	
	2	**L'Entitat de Registre emmagatzema les targetes verges en una ubicació amb accés restringit.**	**OBL**	No avaluat	
	3	**El següent material es custodia a l'interior de la sala d'operacions: PC, impressora de targetes, caixa forta, estoc de targetes generades i la documentació de processos i sistemes.**	**OBL**	No avaluat	
	4	**Els components crítics per a la prestació del servei estan localitzats en un perímetre de seguretat protegit físicament contra la intrusió i es controla l'accés a través d'un perímetre de seguretat i alarma.**	**OBL**	No avaluat	
	5	**L'Entitat de Registre realitza prova de penetració a les infraestructures i la registra.**	**OBL**	No avaluat	
	6	**L'entitat té implementats controls per evitar el compromís o robatori d'informació i de les instal·lacions de processats de la informació.**	**OBL**	No avaluat	
3.2		Seguretat lògica			
	1	**La Entitat de Registre disposa d'un sistema antimalware instal·lat, està actiu i actualitzat (almenys de forma diària).**	**OBL**	No avaluat	
	2	**L'Entitat de Registre dispossa de politiques d'acces, qualitat de contrasenyes i estalvi de pantalles**	**OBL**	No avaluat	
	3	**La Entitat de Registre disposa d'un SAI amb una autonomia suficient per finalitzar un tràmit en condicions segures.**	OPT	No avaluat	

REQUISITS DE SEGURETAT		4	**A la LRA no s'hi ha detectat cap programari instal•lat sense l'aprovació deL Consorci AOC**	**OBL**	No avaluat	
		5	**A la LRA no s'hi ha detectat cap programari instal•lat que permeti accedir-hi de forma remota.**	**OBL**	No avaluat	
		6	**L'entitat de registre únicament fa servir la LRA per realitzar tasques relacionades amb el servei de certificació T-CAT.**	OPT	No avaluat	
		7	**Totes les informacions es tractaran de manera segura segons la seva classificació de risc.**	**OBL**	No avaluat	
		8	**L'Entitat de Registre es protegeix contra l'obsolescència i el deteriorament durant el temps en que s'hagin de conservar els registres.**	**OBL**	No avaluat	
		9	**L'accés a la informació i a les funcions del sistema d'aplicació estan restringits d'acord amb la política d'accés.**	**OBL**	No avaluat	
		10	**Els desplegaments de seguretat que estan disponibles, s'apliquen en un temps raonable.**	**OBL**	No avaluat	
		11	**L'Entitat de Registre es sotmet a simulacres de vulnerabilitats periòdics en adreces IP publicades, privades i sistemes i registra les proves realitzades.**	**OBL**	No avaluat	
		12	**El personal de l'Entitat de Registre s'identifica i autentica abans d'utilitzar aplicacions crítiques relacionades amb el servei.**	**OBL**	No avaluat	
	3.3		Seguretat del personal			
		1	**Els operadors custodien amb diligència les seves targetes d'operador, així com el PIN i el PUK.**	**OBL**	No avaluat	
		2	**En cas de participació de personal extern, aquests han signat una clàusula de confidencialitat amb l'Entitat de Registre**	**OBL**	No avaluat	
		3	**En el cas dels operadors que han causat baixa, el responsable del servei ha procedit a comunicar-ho a Consorci AOC i s'ha revocat el certificat de l'operador en qüestió.**	**OBL**	No avaluat	
		4	**Els operadors no tenen accés a les funcions de confiança (trusted functions) fins que no es compleixen tots els requisits.**	**OBL**	No avaluat	
	3.4		Seguretat de l'arxiu			
		1	**L'entitat de registre disposa de procediment d'arxiu.**	OPT	No avaluat	
		2	**Les targetes inutilitzades es garanteix la destrucció.**	OPT	No avaluat	
		3	**Existeix un protocol o política d'esborrat segur de dades confidencials en dispositius per tal d'evitar l'accés no autoritzat**	**OBL**	No avaluat	

Resum d'avaluació

	Compleix	No compleix	No aplica
Controls obligatoris	0	0	0
Controls optatius	0	0	0

Avaluació: **APTA**

0

PLA D'ACCIÓ	Id. Control	Descripció del control	Id. Acció	Acció	Responsable	Termini Resolució

OBSERVACIONS DE L'ENS	
	Primer. **Segon.** **Tercer.**

Barcelona, dia, mes any

Responsable del servei

Auditor Consorci AOC:

Consorci Administració Oberta de Catalunya

Dades Generals	
Entitat de Registre	
Responsable del servei	
Auditor AOC	
Data auditoria	

Informe d'auditoria d'Entitat de Registre idCAT

Àrees	Id. Control		Control	Tipus Control	Valoració	Evidència / Observació
REQUISITS DE GESTIÓ DOCUMENTAL I ARXIU	1.1.		Tramitació dels expedients			
		1	**Metodologia d'arxiu i traçabilitat**	**OBL**	No avaluat	
		2	**El contingut dels expedients és l'adequat (Sol·licitud d'emissió, acusament de rebuda de correus i còpia del full de lliurament i acceptació de certificats signada pel titular, en els casos en que s'hagi tramitat en paper).**	**OBL**	No avaluat	
		3	**La informació dels expedients seleccionats es correspon amb la informació dels certificats emesos.**	**OBL**	No avaluat	
		4	**Els expedients estan impresos amb paper que compleix la Norma UNE-EN ISO 9706:1999.**	OPT	No avaluat	
	1.2.		Arxiu de gestió			
		1	**Els arxivadors i/o armaris de gestió romanen tancats amb clau quan el personal del servei no està present.**	**OBL**	No avaluat	
		2	**L'accés als arxivadors només es permet al personal autoritzat.**	**OBL**	No avaluat	
	1.3.		Transferència a l'arxiu central			
		1	**Existeix un procediment de transferència d'expedients que defineix la periodicitat, el responsable i el mode d'enviament físic a l'arxiu central.**	OPT	No avaluat	
	1.4.		Arxiu Central			
		1	**Els controls de seguretat física de l'arxiu són adequats.**	**OBL**	No avaluat	
		2	**Metodologia d'arxiu i traçabilitat**	**OBL**	No avaluat	

REQUISITS OPERATIUS	**2.1.**	Documentació Requerida				
	1	**Disposen d'una fitxa de subscriptor actualitzada i ha estat enviada en els darrers 2 anys**		**OBL**	No avaluat	
	2	**Disposen d'una fitxa d'entitat de registre actualitzada i ha estat enviada en els darrers 2 anys**		**OBL**	No avaluat	
	3	**Disposen de termes i condicions on hi consten:**	**Les obligacions dels subscriptors, periode de temps d'arxiu de logs, marc legal i compromis sobre disponibilitat**	**OBL**	No avaluat	
	4	**Disposen de termes i condicions on hi consten:**	**Procediment de queixes i resolució de conflictes**	**OBL**	No avaluat	
	5	**L'entitat informa prèviament als subscriptors i parts interessades sobre els termes i condicions abans d'iniciar la relació contractual**		**OBL**	No avaluat	
	6	**Els termes i condicions es troben disponibles en mitjans no peribles amb un llenguatge entenedor i es poden transmetre electrònicament.**		**OBL**	No avaluat	
	7	**Els serveis han de ser accessibles a tots els sol·licitants**		**OBL**	No avaluat	
	8	**Disposen de polítiques i procediments per a la resolució de conflictes o reclamacions de clients o altres parts interessades**		**OBL**	No avaluat	
	9	**Es diposa de la Fitxa d'identitat i s'ha revisat el compliment**		**OBL**	No avaluat	
	10	**Disposen d'un procediment de gestió d'incidents**		**OBL**	No avaluat	
	11	**Disposen d'un procediment de compliment legal i normatiu (compliance)**		**OBL**	No avaluat	
	12	**Mantenir un llistat actualitzat d'actius d'informació amb l'assignació de la classificació corresponent amb l'avaluació de riscos realitzada.**		**OBL**	No avaluat	
	13	**Es disposa d'un procediment i registre de gestió de canvis per a versions, modificacions i desplegaments.**		**OBL**	No avaluat	
	14	**Existeix un procediment de reinici i recuperació del sistema en cas que falli..**		**OBL**	No avaluat	
	15	**L'Entitat de Registre està alineada amb el pla de continuïtat de l'AOC**		**OBL**	No avaluat	
	2.2.	Formació i repàs de coneixements				
	1	**Tots els operadors han realitzat el curs formatiu d'operador d'entitat de registre idCAT de Consorci AOC.**		**OBL**	No avaluat	
	2	**El responsable del servei mostra coneixement del procediment aprovat per tal de guardar la documentació a l'arxiu de gestió en forma d'expedient.**		**OBL**	No avaluat	
	3	**Es disposa d'una fitxa personal actualitzada amb la formació rebuda del personal involucrat.**		**OBL**	No avaluat	

		4	**Tot el personal (temporal o fixe) disposa de la seva descripció del lloc de treball on hi consta la sensibilització de posició en funció dels drets i nivell d'accés, formació i sensibilització.**	**OBL**	No avaluat	
		5	**L'Entitat de Registre té descrites sancions disciplinàries per aquells treballadors que incompleixin les polítiques o procediments establerts.**	**OBL**	No avaluat	
		6	**L'Entitat de Registre disposa de procediments i processos de gestió alineats amb els de seguretat de la informació.**	**OBL**	No avaluat	
		7	**Tots els operadors han d'estar lliures de conflictes d'interessos que puguin perjudicar la imparcialitat de les operacions del servei.**	**OBL**	No avaluat	
		8	**El personal no tindrà accés a les funcions d'operador del sistema fins que no s'hagin complert tots els controls necessaris.**	**OBL**	No avaluat	
		9	**Tots els operadors mostren coneixement del procediment per registrar i comunicar incidents de seguretat de la informació.**	**OBL**	No avaluat	
		10	**Tots els operadors han rebut una formació sobre actualitzacions sobre noves amenaces i pràctiques de seguretat actuals en els darrers 12 mesos.**	**OBL**	No avaluat	
	3.1.		Seguretat física			
		1	**La sala d'operacions ha de disposar d'un sistema electrònic d'obertura o, com a mínim, d'una porta amb pany i clau. En el cas que això no fos possible, la LRA ha d'estar ubicada en un lloc reservat on només hi tingui accés el personal de l'ER i en cap cas personal aliè al Ens subscriptor.**	OPT	No avaluat	
		2	**L'Entitat de Registre emmagatzema les targetes verges en una ubicació amb accés restringit.**	**OBL**	No avaluat	
		3	**El següent material es custodia a l'interior de la sala d'operacions: PC, impressora de targetes, caixa forta, estoc de targetes generades i la documentació de processos i sistemes.**	**OBL**	No avaluat	
		4	**Els components crítics per a la prestació del servei estan localitzats en un perímetre de seguretat protegit físicament contra la intrusió i es controla l'accés a través d'un perímetre de seguretat i alarma.**	**OBL**	No avaluat	
		5	**L'Entitat de Registre realitza prova de penetració a les infraestructures i la registra.**	**OBL**	No avaluat	
		6	**L'entitat té implementats controls per evitar el compromís o robatori d'informació i de les instal·lacions de processats de la informació.**	**OBL**	No avaluat	
	3.2		Seguretat lògica			
		1	**La Entitat de Registre disposa d'un sistema antimalware instal·lat, està actiu i actualitzat (almenys de forma diària).**	**OBL**	No avaluat	
		2	**L'Entitat de Registre dispossa de politiques d'acces, qualitat de contrasenyes i estalvi de pantalles**	**OBL**	No avaluat	
RETAT		3	**La Entitat de Registre disposa d'un SAI amb una autonomia suficient per finalitzar un tràmit en condicions segures.**	OPT	No avaluat	

REQUISITS DE SEGU						
		4	**Totes les informacions es tractaran de manera segura segons la seva classificació de risc.**	**OBL**	No avaluat	
		5	**L'Entitat de Registre es protegeix contra l'obsolescència i el deteriorament durant el temps en que s'hagin de conservar els registres.**	**OBL**	No avaluat	
		6	**L'accés a la informació i a les funcions del sistema d'aplicació estan restringits d'acord amb la política d'accés.**	**OBL**	No avaluat	
		7	**Els desplegaments de seguretat que estan disponibles, s'apliquen en un temps raonable.**	**OBL**	No avaluat	
		8	**L'Entitat de Registre es sotmet a simulacres de vulnerabilitats periòdics en adreces IP publicades, privades i sistemes i registra les proves realitzades.**	**OBL**	No avaluat	
		9	**El personal de l'Entitat de Registre s'identifica i autentica abans d'utilitzar aplicacions crítiques relacionades amb el servei.**	**OBL**	No avaluat	
	3.3		Seguretat del personal			
		1	**Els operadors custodien amb diligència les seves targetes d'operador, així com el PIN i el PUK.**	**OBL**	No avaluat	
		2	**En cas de participació de personal extern, aquests han signat una clàusula de confidencialitat amb l'Entitat de Registre**	**OBL**	No avaluat	
		3	**En el cas dels operadors que han causat baixa, el responsable del servei ha procedit a comunicar-ho a Consorci AOC i s'ha revocat el certificat de l'operador en qüestió.**	**OBL**	No avaluat	
		4	**Els operadors no tenen accés a les funcions de confiança (trusted functions) fins que no es compleixen tots els requisits.**	**OBL**	No avaluat	
	3.4		Seguretat de l'arxiu			
		1	**L'entitat de registre disposa de procediment d'arxiu.**	OPT	No avaluat	
		2	**Les targetes inutilitzades es garanteix la destrucció.**	OPT	No avaluat	
		3	**Existeix un protocol o política d'esborrat segur de dades confidencials en dispositius per tal d'evitar l'accés no autoritzat**	**OBL**	No avaluat	

Resum d'avaluació

	Compleix	No compleix	No aplica
Controls obligatoris	0	0	0
Controls optatius	0	0	0

Avaluació: **APTA**

0

A D'ACCIÓ	Id. Control	Descripció del control	Id. Acció	Acció	Responsable	Termini Resolució

PL						

OBSERVACIONS DE L'ENS	
	Primer. **Segon.** **Tercer.**

Barcelona, dia, mes any

Responsable del servei

Auditor Consorci AOC:

Consorci
Administració Oberta
de Catalunya

FORMULARI D'AUTOAVALUACIÓ D'ENTITAT DE REGISTRE

Entitat de Registre:

Data:

1.1. Tramitació dels expedients

1.1.1. Hi ha una metodologia d'arxiu i traçabilitat?	SI	NO
En cas afirmatiu, indicar document.		
1.1.2. L'expedient de Sol·licitud d'emissió te acusament de rebuda, una còpia del full de lliurament, i acceptació de certificats signada pel titular?		
1.1.3. La informació dels expedients seleccionats es correspon amb la informació dels certificars emesos.	SI	NO
1.1.4. Els expedients impresos amb paper compleixen la Norma Une-EN ISO-9076?	SI	NO

1.2. Arxiu de Gestió

1.2.1. Es tanquen amb clau els arxivadors i/o armaris de gestió quan el personal de servei no està present?	SI	NO
1.2.2. El personal autoritzat es l'únic que pot accedir als arxivadors?	SI	NO

1.3. Transferència a l'arxiu central

1.3.1. Existeix un procediment de transferència d'expedients que defineix la periodicitat, el responsable i el mode d'enviament físic a l'arxiu central?*	SI	NO
*En el cas de que la resposta sigui NO, indicar quins dels requeriments no es compleixen		

1.4. Arxiu Central

1.4.1. Els controls de seguretat física de l'arxiu són adequats?	SI	NO
1.4.2. Hi ha una metodologia d'arxiu i una traçabilitat?	SI	NO

2.1. Documentació Requerida

2.1.1. Es disposa d'una fitxa de subscriptor actualitzada i ha estat enviada en els darrers 2 anys?*	SI	NO
* En cas que la resposta sigui no, indicar per què		
2.1.2. Es disposa d'una fitxa d'entitat de registre actualitzada i ha estat enviada els darrers 2 anys?*	SI	NO
* En cas que la resposta sigui no, indicar per què		
2.1.3. Es disposa de termes i condicions on hi consten:		
a) Les obligacions dels subscriptors.	SI	NO
b) El periode de temps d'arxiu de logs.	SI	NO
c) Marc Legal.	SI	NO
d) Compromís sobre disponibilitat.	SI	NO
2.1.4. Es disposa de termes i condicions on hi consta un procediment de queixes i resolució de conflictes?	SI	NO
2.1.5. L'entitat informa prèviament als subscriptors i parts interessades sobre els termes i condicions abans d'iniciar la relació contractual.	SI	NO
2.1.6. Els termes i condicions es troben disponibles en mitjans no peribles amb un llenguatge entenedor i es poden transmetre electrònicament.	SI	NO

2.1.7. Els serveis son accessibles a tots els sol·licitants.	SI	NO
2.1.8. Es disposa de polítiques i procediments per a la resolució de conflictes o reclamacions de clients o altres parts interessades?*	SI	NO
*En cas afirmatiu, indicar procediments.		
2.1.9. Es disposa de una Fitxa d'identitat i s'ha revisat el compliment	SI	NO
2.1.10. Es disposa d'un procediment de gestió d'incidents?	SI	NO
2.1.11. Es disposa d'un procediment de compliment legal i formatiu (compliance)?	SI	NO
2.1.12. Es manté un llistat d'actius actualitzat amb l'assignació de classificació d'informació corresponent i una avaluació de riscos dels mateixos?	SI	NO
2.1.13. Es disposa d'un procediment i registre de gestió de canvis per a versions, modificacions i desplegaments?	SI	NO
*En cas afirmatiu, indicar procediment.		
2.1.14. Existeix un procediment de reinici i recuperació del sistema en cas que falli?*	SI	NO
*En cas afirmatiu, indicar procediment.		
2.1.15. L'Entitat de Registre està alineada amb el pla de continuïtat de l'AOC?	SI	NO

2.2. Formació i repàs de coneixements

2.2.1. Han realitzat tots els operadors el curs formatiu d'operador d'entitat de registre T-CAT de Consorci AOC?	SI	NO
2.2.2. El responsable del servei mostra coneixement del procediment aprovat per tal de guardar la documentació a l'arxiu de gestió en forma d'expedient?	SI	NO

2.2.3. Es disposa d'una fitxa personal actualitzada amb la formació rebuda del personal involucrat?	SI	NO
2.2.4. Disposa tot el personal (temporar o fixe) de la seva descripció del lloc de treball on hi consta la sensibilització de posició en funció dels drets, nivell d'accés i formació?	SI	NO
2.2.5. Disposa l'Entitat de Registre de descripcions de les sancions disciplinàries per aquells treballadors que incompleixin les polítiques o procediments establerts?	SI	NO
2.2.6. Disposa L'Entitat de Registre de procediments i processos de gestió alineats amb els de seguretat de la informació?	SI	NO
*En cas afirmatiu, indicar procediment.		
2.2.7. Estan tots els operadors lliures de conflictes d'interessos que puguin perjudicar la imparcialitat de les operacions del servei?	SI	NO
2.2.8. Té el personal accés a les funcions d'operador del sistema abans que es completin tots els controls necessaris?	SI	NO
2.2.9. Mostren tots els operadors coneixement del procediment per registrar i comunicar incidents de Seguretat de la Informació?	SI	NO
2.2.10. Han rebut tots els operadors una formació sobre actualitzacions sobre noves amenaces i pràctiques de seguretat actuals en els darrers 12 mesos?	SI	NO

3.1. Seguretat física

3.1.1. Disposa la sala d'operacions d'un sistema electrònic d'obertura o, como a mínim, d'una porta amb pany i clau?*	SI	NO
* En cas que la resposta sigui NO, indicar de qué es disposa.		
3.1.2. Emmagatzema l'Entitat de Registre les targetes verges en una ubicació amb accés restringit?	SI	NO
3.1.3. Es custodia el següent material a l'interior?		
a) PC	SI	NO
b) Impressora de targetes	SI	NO

c) Caixa Forta	SI	NO
d) Estoc de Targetes generades	SI	NO
e) Documentació de Processos i Sistemes	SI	NO
3.1.4. Están els components crítics per a la prestació del servei localitzats en un perímetre de seguretat protegit físicament contra la intrusió i es controla l'accés a través d'un perímetre de seguretat i alarma?*	SI	NO
* En cas que la resposta sigui NO, descriure les mesures de seguretat de que es disposa		
3.1.5. L'Entitat de Registre realitza i registra proves de penetració a les infraestructures?	SI	NO
3.1.6. L'entitat té implementats controls per evitar el compromís o robatori d'informació i de les instal·lacions de processats de la informació?	SI	NO

3.2. Seguretat Lògica

3.2.1. Disposa la Entitat de Registre d'un sistema antimalware instal-lat?	SI	NO
a) Està actiu?	SI	NO
b) S'actualitza al menys de forma diaria?	SI	NO
3.2.2. Disposa la Entitat de Registre de polítiques d'acces, qualitat de contrasenyes i estalvi de pantalles?	SI	NO
3.2.3. Disposa la Entitat de Registre d'un SAI amb una autonomia suficient per finalitzar un tràmit en condicions segures?	SI	NO
3.2.4. A la LRA s'ha detectat programari instal•lat sense l'aprovació del Consorci AOC	SI	NO
3.2.5. A la LRA s'ha detectat programari instal•lat que permeti accedir-hi de forma remota.	SI	NO
3.2.6. L'Entitat de registre fa servir la LRA unicament per realitzar tasques relacionades amb el servei de certificació T-CAT?*	SI	NO
* En cas que la resposta sigui NO, descriure quines altres tasques realitza amb la LRA		

3.2.7. Es tracten de manera segura segons la seva classificació de risc totes les informacions?	SI	NO
3.2.8. Es protegeix l'Entitat de Registre contra l'obsolescencia i la deterioració durant el temps en que s'hagin de conservar els registres?	SI	NO
3.2.9. Están l'accés a l'informació i a les funcions del sistema d'aplicació restringides d'acord amb la política d'accés?	SI	NO
3.2.10. S'apliquen en un temps raonable els desplegaments de seguretat disponibles?	SI	NO
3.2.11. Es somet l'Entitat de Registre a simulacres de vulnerabilitat periòdics en adreçes IP publicades, privades i sistemes i registra es proves realitzades?	SI	NO
3.2.12. El personal de l'Entitat de Registre s'identifica i autentica abans d'utilitzar aplicacions crítiques relacionades amb el servei?	SI	NO

3.3. Seguretat del Personal

3.3.1. Els operadors custodien amb diligència les seves targetes d'operador, així com el PIN i el PUK?	SI	NO
3.3.2. En cas de participació de personal extern, aquests signen una clàusula de confidencialitat amb l'Entitat de Registre?	SI	NO
3.3.3. En el cas dels operadors que han causat baixa, el responsable del servei ha procedit a comunicar-ho a Consorci AOC i s'ha revocat el certificat de l'operador en qüestió?	SI	NO
3.3.4. Els operadors tenen accés a les funcions de confiança (trusted functions) abans de que es compleixen tots els requisits?	SI	NO

3.4. Seguretat de l'arxiu

3.4.1. L'entitat de registre disposa de procediment d'arxiu?	SI	NO
3.4.2. Es garanteix la destrucció de les targetes inutilitzades?	SI	NO
3.4.3. Existeix un protocol o política d'esborrat segur de dades confidencials en dispositius per tal d'evitar l'accés no autoritzat?	SI	NO

Signem la present declaració a data del document.

Nom de la persona que signa:

Lloc de treball de la persona que signa:

Consorci
Administració Oberta
de Catalunya

Auditories relacionades amb SCD:

- ER T-CAT
- ER idCAT
- ER d'identitats (Ens subscriptors)

Generalitat de Catalunya

LOCALRET

Realitzat per:
Versió:
Data: 09/07/2024~~21/06/2019~~
Arxiu: D1153 Auditoria de conformitat.doc

Index

1 Objecte i abast

L'objecte d'aquest document és desenvolupar els requisits de les Auditories relacionades amb els organismes que executant part Servei de Certificació Digital concretament en els àmbits de :

- **Entitats de registre T-CAT**: és un ens o departament que col·labora amb el Consorci AOC en la l'emissió de certificats digitals a les administracions públiques catalanes.
- **Entitats de Registres idCAT** : és un ens o departament que col·labora amb l'AOC, en el registre de les identitats digitals per a la ciutadania, concretament per a emetre i gestionar certificats idCAT i l'idCAT al mòbil.
- **Entitats de registre o Ens subscriptors:** és un ens o departament que col·labora amb el Consorci AOC en els tràmits d'identificació, registre i autenticació per a l'emissió de certificats digitals, seguint els procediments i les relacions amb els titulars dels certificats.

2 Programació d'auditories

2.1 Freqüència d'auditoria de conformitat

El Consorci AOC, com a prestador de serveis de certificació, té l'obligació de realitzar periòdicament una auditoria de conformitat a les seves Entitats de Registre i ens subscriptor per a provar que compleix amb els requisits de seguretat, arxiu i operacionals marcats en la documentació del servei.

Es procedirà a un mostreig que permeti de forma bianual la revisió de la totalitat de les entitats que han fet us del servei SCD.

L'execució d'aquestes auditories es realitzarà de manera virtual o presencial segons programació anual. S'auditarà presencialment les Entitats de Registre T-CAT i idCAT que per criteris de volum d'emissions, incidències o altres factors que ho requereixen.

2.2 Estudi inicial de l'entorn a auditar

Per a materialitzar les auditories caldrà realitzar una sèrie de tasques prèvies:

- Revisió de la documentació actual
    - Comprovar que existeix la fitxa o alta del servei al dia
    - Nombre de certificats emesos
    - Data de la darrera auditoria i resultats (en el cas que n'hi hagi)
    - Revisió de qualsevol canvi que hagi pogut afectar al servei.
    - Revisió i tria dels certificats a auditar
    - Revisió de les possibles dades errònies en les dades dels titulars dels certificats.
    - Llistat d'incidències sofertes
    - Llistat del personal que participa en els processos del Servei de Certificació Digital
    - Verificació de l'existència d'un arxiu central on romanguin arxivats els documents relacionats amb el SCD i control de la documentació i registres.
    - Informe de revisió per la direcció, on s'especifiqui el següent:
        - Resultats d'auditories internes i externes
        - Retroalimentació de parts interessades
        - Retroalimentació del mecanisme per mantenir la imparcialitat
        - Estat de les accions preventives i correctives
        - Accions de seguiment provinents de revisions prèvies per part de la direcció
        - Compliment d'objectius
        - Canvis que podrien afectar al sistema de gestió
        - Queixes i apel·lacions
        - Accions i decisions relatives a :
            - Millora de la eficàcia del sistema de gestió i dels seus processos
            - Millora de l'organisme de certificació en relació al compliment de norma
            - La necessitat de recursos

2.3 Pla d'auditories

Anualment l'AOC procedirà a una programació de entitats a auditar que contemplarà el requeriments legals i el mostreig definit en el punt 2.1.

Posteriorment s'executarà un pla d'auditoria on s'informarà als centres seleccionats.

Aquest pla d'auditoria haurà d'incloure els següents punts:

- Objectiu i abast
- Criteris d'auditoria

- Equip auditor
- Documents de referència
- Agenda amb temps d'inici o durada
- Temes de confidencialitat
- Riscos de l'auditoria
- Instruccions de resolució i seguiment

S'haurà de comunicar amb anterioritat 30 dies al centre.

3 Execució d'auditories

3.1 Relació d'elements objecte d'auditoria

- Termes i condicions: Posar a disposició dels subscriptors, les entitats de registre i parts interessades els termes i condicions de cadascun dels serveis prestats. Aquests termes i condicions especificaran:
  - Les obligacions del subscriptor i les entitats de registre, si hi ha,
  - El període de temps que es guarden els logs del servei de confiança
  - Les limitacions de responsabilitat
  - Marc legal aplicable
  - Procediment de queixes i resolució de conflictes
  - Informació de contacte del servei de confiança
  - Compromís sobre la disponibilitat

  Cal informar als subscriptors, les entitats de registre i a les parts interessades dels termes i condicions abans d'iniciar la relació contractual. A més, aquests termes i condicions han d'estar disponibles a través de mitjans de comunicació no peribles, amb un llenguatge entenedor i que es puguin transmetre electrònicament.
- Operació i gestió del servei
  - Els serveis han de ser accessibles a tots els sol·licitants, les activitats dels quals estan dins del seu camp d'operació declarat i que accepten complir les seves obligacions especificades als termes i condicions del servei.
  - Disposar de polítiques i procediments per a la resolució de conflictes o reclamacions de clients o altres parts interessades
  - Contracte en vigor amb l'AOC.
- Recursos humans involucrats: L'ens s'ha d'assegurar que el personal que dona el servei és responsable i dona confiança al servei donat.
  - El personal estarà qualificat per fer la feina encomanada i haurà rebut formació sobre seguretat i protecció de dades personals adequades al servei ofert i el lloc de treball.

- Es disposarà d'una fitxa de personal actualitzada amb la formació rebuda (coneixement, experiència i qualificacions) o experiència en el lloc de treball que s'anirà actualitzant cada any, en funció d'actualitzacions sobre noves amenaces o noves pràctiques de seguretat.
- Es descriuran sancions disciplinàries per aquells treballadors que incompleixin les polítiques o procediments establerts.
- Les funcions de seguretat i les responsabilitats estaran descrites clarament en la descripció dels llocs de treball que estaran disponibles per a tot el personal implicat. Les funcions de confiança, de les que depèn la seguretat de la operació del servei, han d'estar clarament identificades. Les funcions de confiança seran nomenades per la direcció i seran acceptades per la direcció i per la persona implicada.
- Tot el personal (temporal o fixe) disposarà de la seva descripció del lloc de treball on hi constarà la sensibilitat de posició en funció del drets i nivell d'accés, formació i sensibilització.
- Es disposarà de procediments i processos de gestió alineats amb els de seguretat de la informació.
- Tot el personal amb funcions de confiança han d'estar lliures de conflictes d'interessos que puguin perjudicar la imparcialitat de les operacions del servei.
- Les funcions de confiança inclouen:
  - Operador del sistema: Responsable per operar el sistema de confiança en el dia a dia. Autoritzat per realitzar la còpia de seguretat.
- El personal no tindrà accés a les funcions de confiança fins que no s'hagin complert tots els controls necessaris.

- Gestió d'actius: L'ens s'haurà d'assegurar del nivell apropiat de protecció dels actius, incloent els actius d'informació.
  - Mantenir un llistat actualitzat d'actius d'informació amb l'assignació de la classificació corresponent amb l'avaluació de riscos realitzada.
  - Tots els materials es tractaran de manera segura segons la seva classificació de risc. Els materials que continguin dades sensibles es destruiran de manera segura quan ja no siguin necessaris.
- Control d'accés digital: L'accés al sistema estarà limitat al personal autoritzat.
  - L'accés a la informació i a les funcions del sistema d'aplicació han d'estar restringits d'acord amb la política d'accés.
  - El personal de l'ens s'ha d'identificar i autenticar abans d'utilitzar aplicacions crítiques relacionades amb el servei.
  - El personal de l'ens es responsable de les seves activitats.
  - Ha d'existir un protocol o política d'esborrat segur de dades confidencials en dispositius per tal d'evitar l'accés no autoritzat.
- Control d'accés físic: S'ha de controlar l'accés físic als components del sistema de l'ens, la seguretat dels quals és crítica per a la provisió del servei de confiança i minimitzar els riscos relacionats amb la seguretat física.
  - Accés físic limitat als components del sistema de l'ens que són crítics per a la prestació del servei.

- S'han d'implementar controls per evitar la pèrdua, dany o compromís d'actius i interrupció de les activitats
- S'han d'implementar controls per evitar el compromís o robatori d'informació i de les instal·lacions de processats de la informació.
- Els components que són crítics per a la prestació del servei han d'estar localitzats en un perímetre de seguretat protegit físicament contra la intrusió i s'ha de controlar l'accés a través d'un perímetre de seguretat i alarma.

- Seguretat operacional: L'ens ha d'utilitzar sistemes de confiança i productes protegits contra modificacions i s'ha d'assegurar de la seguretat tècnica i fiabilitat dels processos realitzats per ells.
  - Cal aplicar un procediment i registre de gestió de canvis per a versions, modificacions i correccions de software.
  - La integritat dels sistemes de l'ens han d'estar protegits contra virus, software maliciós i software no autoritzat.
  - Els materials utilitzats en els sistemes de l'ens s'han de gestionar de manera segura per protegir -los de danys, robatoris, accessos no autoritzats i obsolescència.
  - S'han de protegir contra la obsolescència i el deteriorament, els materials utilitzats durant el temps en què s'hagin de conservar els registres.
  - S'han d'implementar i establir els procediments per a les funcions administratives i de confiança que impacten a la provisió dels serveis.
  - L'ens ha d'aplicar procediments per assegurar-se del següent:
    - Els desplegaments de seguretat que estan disponibles s'apliquen en un temps raonable.
    - No s'apliquen desplegaments de seguretat que introdueixen vulnerabilitats o inestabilitats majors que els beneficis que puguin aportar.
    - Es documenten les raons per les quals no d'aplicat un desplegament de seguretat.
- Seguretat de les xarxes: L'ens ha de protegir la seva xarxa i els seus sistemes dels atacs.
    - L'ens mantindrà tots els sistemes que són crítics per a l'operació de l'ens en una o més zones segures.
    - L'ens ha de sotmetre's o realitzar un escàner de vulnerabilitat periòdic en adreces IP publicades i privades identificades per l'ens i registrar proves que cada persona o entitat realitzava cada escaneig de vulnerabilitat amb les habilitats, les eines, la competència, el codi ètic i la independència necessari per proporcionar un informe fiable.
    - L'ens s'ha de sotmetre a una prova de penetració en els seus sistemes en la instal·lació i després de la infraestructura o les actualitzacions o modificacions de les aplicacions que determini l'ens com a significatives. L'ens registrarà proves que cada prova de penetració va ser realitzada per una persona o entitat amb les habilitats, les eines, la competència, el codi ètic i la independència necessàries per proporcionar un informe fiable.

- Gestió d'incidents: S'ha de controlar l'activitat del sistema relacionada amb l'accés als sistemes informàtics, l'ús de sistemes informàtics i les sol·licituds de servei.
    - Les activitats de seguiment haurien de tenir en compte la sensibilitat de qualsevol informació recollida o analitzada
    - Les activitats anormals del sistema que indiquen una possible vulneració de seguretat, inclosa la intrusió a la xarxa de l'ens, s'han de detectar i informar com a alarmes.
    - Els sistemes de TI de l'ens han de supervisar els següents esdeveniments:
        - Posada en marxa i apagada de les funcions de registre; i
        - Disponibilitat i utilització dels serveis necessaris amb la xarxa de l'ens.
    - L'ens ha d'actuar de manera oportuna i coordinada per respondre ràpidament a incidents i limitar l'impacte de les violacions de la seguretat. L'ens ha de designar personal de rol de confiança per fer un seguiment de les alertes de esdeveniments de seguretat potencialment crítics i garantir que es registrin incidents rellevants d'acord amb els procediments de l'ens.
    - L'ens ha d'establir procediments per notificar a les parts apropiades d'acord amb les normes reguladores aplicables de qualsevol incompliment de la seguretat o pèrdua d'integritat que tingui un impacte significatiu en el servei de confiança prestat i en les dades personals mantingudes en ell, dins de les 24 hores posteriors al moment en que s'identifica l'incompliment.
    - Quan l'incompliment de la seguretat o pèrdua d'integritat pugui afectar negativament a una persona física o jurídica a la qual s'ha prestat el servei fiduciari, l'ens també notificarà a la persona física o jurídica l'incompliment de la seguretat o la pèrdua d'integritat sense demora indeguda .
    - S'han de controlar els sistemes de l'ens, inclosa la supervisió o la revisió periòdica dels registres d'auditoria per identificar evidències d'activitat maliciosa que impliquen mecanismes automàtics per processar els registres d'auditoria i personal d'alertes de possibles esdeveniments de seguretat crítics.
    - L'ens abordarà qualsevol vulnerabilitat crítica que no s'hagi tractat prèviament pel mateix, dins del termini de 48 hores després del seu descobriment. Si això és efectiu en funció de l'efecte en termes de costos, l'ens ha de crear i implementar un pla per mitigar la vulnerabilitat o documentarà la base per la qual la vulnerabilitat no cal ser tractada.
    - S'han d'utilitzar els procediments d'informació i resposta dels incidents de manera que es minimitzi el dany causat per incidents de seguretat i mal funcionament.

- Alineació amb el Pla de continuïtat de negoci de l'AOC: L'ens ha de tenir definit i mantenir un pla de continuïtat que promulgarà en cas de desastre.
- Compliment legal i normatiu: L'ens s'ha d'assegurar que opera dins el marc legal aplicable.

  - Procediment de compliment de marc legal on es pugui demostrar com es gestiona el marc legal.
  - L'ens s'ha d'assegurar que els serveis són accessibles a persones amb discapacitat.
  - Compliment del marc legal vigent en protecció de dades personals. Adequació al nou Reglament Europeu de Protecció de Dades.
- Gestió de la identificació:
- Gestió del canvi: Procediment transversal on es planifiquin els canvis, es registrin i es dugui un seguiment.

3.2 Pautes de l'auditoria virtual

Mirar els annexos específics per a cada ens.

- Fer mostreig dels certificats personals generats. establir un valor no superior al 10% o un mínim de 10 certificats.
- Fer un mostreig dels certificats de dispositiu i aplicació generats (casos d'ER T-CAT i ens subscriptor), no superior al 10% o un mínim de 10 certificats.
- Enviar un correu al responsable del Servei de l'ens amb l'informe d'auditoria per omplir i signar i amb els noms dels titulars dels fulls de lliurament sol·licitats. Caldrà que ens enviïn aquesta documentació escanejada al correu electrònic indicat.
- L'auditora haurà de comprovar que les dades del certificat generat són les mateixes que el certificat sol·licitat o que el DNI. En els casos de full de lliurament de T-CAT es comprovarà mitjançant l'aplicació que el full de lliurament no s'ha imprès en el moment de l'auditoria si no quan es va realitzar el certificat
- Comprovar la seguretat del tractament de dades personals en compliment de la legislació vigent.

3.3 Pautes de l'auditoria presencial

Mirar els annexos específics per a cada ens.

- Concertar la visita per a la realització de l'auditoria amb el responsable del Servei, sol·licitant la participació de tots els rols implicats.
- Fer un mostreig dels certificats personals generats, entre un 5% i un 10% del total.
- Fer un mostreig dels certificats de dispositiu i aplicació generats (casos d'ER T-CAT i ens subscriptor), entre un 6% i un 10%.
- Sol·licitar al responsable del servei la documentació del mostreig per a analitzar.
- L'auditora haurà de comprovar que les dades del certificat generat són les mateixes que el certificat sol·licitat o que el DNI o altres documents identificatius. En els casos de full de lliurament de T-CAT es comprovarà que estan degudament arxivats.
- Comprovar la seguretat del tractament de dades personals en compliment de la legislació vigent.

3.4 Elaboració dels informes d'auditoria

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

1.- Completar *Cheking* de seguiment.
2.- Realització de l'informe tot indicant quines son les no conformitats trobades i les evidències que ho demostren.
3.- Creació de les fitxes amb els plans d'acció per corregir els errors. Cal crear una fitxa per problema trobat.
4.- Enviar l'informe
5.- Comunicar a l'ER o ens subscriptor, les debilitats significatives i les recomanacions oportunes.
6.- Indicar a l'ER o ens subscriptor com s'actuarà des del Consorci AOC per realitzar el seguiment de les recomanacions.

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

Els informes de resultats de les auditories seran lliurats pel Consorci AOC, en un termini màxim de 25 dies després de l'execució de l'auditoria, per a la seva avaluació i gestió diligent. En cas d'una no conformitat en termes de protecció de dades personals, s'haurà d'informar a al Delegat de Protecció de Dades per que informi a l'AGPD.
Per altres no conformitats, s'haurà de descriure les actuacions a fer per esmenar la no conformitat, marcar un responsable i un termini de resolució coherent.

3.6 Finalització d'auditoria

A la recepció de les correccions, l'auditor avaluarà la conformitat de les accions executades per garantir la correcció de les desviacions.

S'haurà de tenir especial compte per:

1- Establir mesures per controlar el progrés de les no conformitats greus.
2- Realitzar les revocacions d'ofici dels certificats emesos de manera errònia. (Enviant mail al subscriptor).
3- En cas que l'ER idCAT no faci el recull dels DNI's caldrà que enviïn el correu de plantilla per a que el subscriptor el porti a l'ER. En cas que no el porti en 90 dies, el Consorci AOC procedirà a la revocació d'ofici d'aquell certificat.

Un cop avaluat l'auditor considerarà tancat el procés d'auditoria.

4 Normativa aplicable

- UNE-EN-ISO 19011:2011 Directrices para la auditoria de los sistemas de gestión.
- UNE-EN-ISO/IEC 17065:2012 Evaluación de la conformidad. Requisitos para organismos que certifican productos, procesos y servicios.
- Reglament (UE) Nº 910/2014 del Parlament Europeu i del Consell de 23 de juliol de 2014 relatiu a la identificació electrònica i els serveis de confiança per a les transaccions electròniques en el mercat interior i per la que es deroga la Directiva 1999/93/CE.
- DIRECTIVA (UE) 2016/1148 DEL PARLAMENT EUROPEU I DEL CONSELL de 6 de juliol de 2016 relativa a les mesures destinades a garantir un elevat nivell comú de seguretat de les xarxes i sistemes d'informació a la Unió
- ETSI EN 319 401 Electronic Signatures and Infrastructures (ESI); General Policy Requirements for Trust Service Providers
- ETSI EN 319 403 Electronic Signatures and Infrastructures (ESI); Trust Service Provider Conformity Assessment-Requirements for conformity assessment bodies assessing Trust Services Providers
- I tota la relacionada amb la prestacions de serveis de certificació

5 Relació de registres

Plantilla de correu electrònic amb la planificació de l'auditoria

Model d'informe d'auditoria

Checking d'auditoria

Consorci
Administració Oberta
de Catalunya

INFORME D'AUDITORIA DE CONFORMITAT

ENTITAT DE REGISTRE

data

1. DADES DE L'ORGANITZACIÓ

NOM:

ADREÇA:

RESPONSABLE:

OBJECTE:

DATA DE REALITZACIÓ:

DIRECCIONS DE L'ORGANITZACIÓ:

2. ABAST DE L'AUDITORIA

Seus:

3. APLICABILITAT

4. EQUIP AUDITOR

AUDITOR CAP:
AUDITOR:

5. DOCUMENTACIÓ DE REFERÈNCIA

6. MOSTRA AUDITADA

Total personal		**Grau de confiança**	**%**
Personal auditat			
Tipus de certificats		**Grau de confiança**	**%**
Tipus auditats			

7. NO CONFORMITATS

DESCRIPCIÓ DE LA NO CONFORMITAT	Àrea afectada

8. OBSERVACIONS

DESCRIPCIÓ DE LES OBSERVACIONS

9. OPORTUNITATS DE MILLORA APORTADES PER L'AUDITOR

DESCRIPCIÓ DE LES PROPOSTES DE MILLORA

10. RESULTAT

1. L'organització es quedarà amb una copia de l'informe.
2. Les no conformitats han estat aclarides i enteses.
3. Tenint en compte les no conformitats constatades i indicades en aquest informe, l'entitat de registre es compromet a presentar accions correctives.
4. L'equip auditor informa que aquesta auditoria s'ha realitzat a través d'un mostreig pel que poden existir altres no conformitats no identificades en aquest informe.
5. Les no conformitats es refereixen a incompliments dels requisits de la Regulació eIDAS a través de les normes ETSI.
6. OPINIÓ DE L'AUDITOR: L'auditora considera **adequada la situació actual**.

11. MODIFICACIONS DE L'ABAST

No consten modificacions a l'abast.

Lloc:
Data:

Signatura/s Auditor/s

Signatura del representant de l'organització

ANNEX xxx VOLUMETRIES D'EMISSIÓ DE CERTIFICATS

	ANY									
TIPUS DE CERTIFICAT	**2014**	**2015**	**2016**	**2017**	**2018**	**2019**	**2020**	**2021**	**2022**	**2023**
Certificats personal T-CAT	16.805	18.967	20.793	19.766	28.338	17.534	16.259	17.646	21.026	36.378
Certificat personal T-CAT urgents	792	1.179	1.320	1.692	1.851	1.389	1.240	1.806	1.695	3.723
T-CAT P	285	1.171	1.461	2.990	5.162	5.588	9.962	12.045	15.099	37.027
TCAT P urgent	9	56	81	142	206	371	1.256	751	628	3.363
TCAT P classe 2	0	2	3	3	12	0	5	28	12	47
TCAT P classe 2 urgent	0	0	0	0	0	0	2	0	2	2
certificat operador idcat	436	483	406	490	504	570	610	720	750	789
certificat operador T-CAT	143	137	151	101	141	75	67	85	11	97
Certificat classe 2	4.409	7.001	4.140	4.098	505	20	37	23	58	169
Certificat operador Classe 2	32	15	15	7	44	14	34	40	32	24
Certificat idCAT	34.424	33.076	52.099	69.588	88.225	109.552	191.360	298.600	277.562	321.311
certificat seu electrònica (*)	66	51	47	59	118	no aplica	no aplica	no aplica	no aplica	no aplica
certificat seu electrònica urgent (*)	11	13	15	13	41	no aplica	no aplica	no aplica	no aplica	no aplica
certificat CDS (*)	739	902	1.017	991	1.227	no aplica	no aplica	no aplica	no aplica	no aplica
certificat CDS urgent (*)	51	59	65	33	39	no aplica	no aplica	no aplica	no aplica	no aplica
certificat EV (*)	33	27	32	47	56	no aplica	no aplica	no aplica	no aplica	no aplica
certificat EV urgent (*)	1	2	6	8	6	no aplica	no aplica	no aplica	no aplica	no aplica
Certificat CDA	133	144	181	277	249	137	223	294	248	136
Certificat CDA urgent	5	13	25	33	25	17	29	43	53	19
Certificat CDANM	386	616	555	661	845	948	770	753	958	838

Certificat CDANM urgent	38	66	65	82	75	77	29	33	75	77
Certificat pseudònim	0	0	0	0	119	178	180	319	773	1.661
Certificat pseudònim urgent	0	0	0	0	0	0	0	0	0	0
Certificat representant	0	0	0	0	21	75	82	39	68	250
Certificat representant urgent	0	0	0	0	0	0	0	0	0	0

(*) els certificats marcats es van deixar d'emetre al 2018
(**) cal tenir en compte la variabilitat depenent d'entre d'altres dels anys electorals.

ANNEX xxx Entitats de Registre T-CAT

Consorci AOC

Diputació de Tarragona

Ajuntament de Castelldefels

Ajuntament de Girona

Ajuntament de Lleida

Ajuntament de Vilanova i la Geltrú

Consell Comarcal de l'Alt Penedés

Consell Comarcal de l'Alt Urgell

Consell Comarcal del Baix Ebre

Consell Comarcal de la Conca de Barberà

Consell Comarcal de la Garrotxa

Consell Comarcal d'Osona

Consell Comarcal del Pallars Sobirà

Consell Comarcal de la Ribera d'Ebre

Consell Comarcal del Ripollès

Consell Comarcal del Segrià

Consell Comarcal de la Selva

Consell Comarcal del Tarragonès

Consell Comarcal de la Terra Alta

Organisme de Gestió Tributària de la DIBA

Consell Comarcal del Pla de l'Estany

Ajuntament de Sant Feliu de Llobregat

Ajuntament de Mollet del Vallés

Consell Comarcal del Baix Camp

Consell Comarcal de la Segarra

Consell Comarcal de l'Alt Camp

Ajuntament de Tarragona

Ajuntament de Reus

Ajuntament de Manresa

Ajuntament de Badalona

Consell Comarcal del Maresme

Consell Comarcal del Vallés Oriental

Consell Comarcal de l'Anoia

Consell Comarcal del Pla d'Urgell

Consell Comarcal de la Noguera

Consell Comarcal del Berguedà

Consell Comarcal del Baix Empordà

Consell Comarcal del Pallars Jussà

Consell Comarcal de l'Urgell

Consell Comarcal del Vallés Occidental

Consell Comarcal del Garraf

Consell Comarcal del Montsià

Ajuntament de Sabadell

Consell Comarcal de l'Alt Empordà

Consell Comarcal de l'Alta Ribagorça

Consell Comarcal del Priorat

Consell Comarcal del Baix Penedès

Consell Comarcal de les Garrigues

Conselh Generau d'Aran

Consell Comarcal del Solsonés

Consell Comarcal del Bages

Consell Comarcal de la Cerdanya

Consell Comarcal del Gironés

Ajuntament de Cerdanyola del Vallés

Ajuntament de Mataró

Ajuntament de Cornellà de Llobregat

Consell Comarcal del Baix Llobregat

CTTI

Autoritat Catalana de Protecció de Dades

CESICAT

Mossos d'Esquadra

UPC

Universitat de Lleida

Universitat Pompeu Fabra

Universitat de Barcelona

Universitat Rovira i Virgili

Parlament de Catalunya

Consell Comarcal del Moianès

(*) aquest llistat es a data juny de 2024 i pot variar al llarg del temps.

ANNEX Entitats de Registre idCAT

Ajuntament de Castell-Platja d'Aro
Ajuntament de Pallejà
Ajuntament de Sabadell. SAC Despatx Lluch
Ajuntament de la Cellera de Ter
Ajuntament de Manlleu - Oficines centrals
Ajuntament de Mataró
Ajuntament de Mataró
Ajuntament de Mataró
Ajuntament de Mataró
Ajuntament de Palafolls
Ajuntament de Sils
Consell Comarcal del Pla de l'Estany
Departament de Cultura- Palau Marc
Institut Municipal d'Hisenda
OAC de la Generalitat de Catalunya a la Cerdanya
OAC de la Generalitat de Catalunya a Lleida
OFICINA D'ATENCIÓ A LES EMPRESES (OAEM)
Oficina d'Atenció al Ciutadà - Districte de Nou Barris
Oficina d'Atenció Ciutadana - Districte de Ciutat Vella
Oficina d'Atenció Ciutadana - Districte de Gràcia
Oficina d'Atenció Ciutadana - Districte de l'Eixample
Oficina d'Atenció Ciutadana - Districte de Les Corts
Oficina d'Atenció Ciutadana - Districte de Sant Martí
Oficina d'Atenció Ciutadana - Districte de Sarrià-Sant Gervasi
Oficina d'Atenció Ciutadana - Districte d'Horta- Guinardó
Sant Andreu, Oficina d'Atenció al Ciutadà - Districte de
TRESORERIA MUNICIPAL
Ajuntament de Mataró
Oficina d'Atenció Ciutadana - Districte de Sants- Montjuïc
Oficina d'Atenció Ciutadana - Plaça Sant Miquel
OFICINA D'ATENCIÓ CIUTADANA MONUMENTAL
Ajuntament de Sant Adrià de Besòs
Ajuntament de Barberà del Vallès
Ajuntament de Sant Cugat del Vallès
Ajuntament de Vilablareix
Cateb - Oficina Vilafranca
Cateb - Oficina Barcelona
Cateb - Oficina Terrassa
Cateb - Oficina Mataró - Cateb
Cateb - Oficina Manresa
Cateb - Oficina Granollers

Cateb - Oficina Vic
UAB - Arxiu General i Registre
Ajuntament de Badalona
Ajuntament de Begues
Ajuntament de Calonge de Segarra
Ajuntament de Castelló d'Empúries
Ajuntament de Sant Celoni
Ajuntament d'El Bruc
Consell Comarcal del Moianès
Garraf, Consell Comarcal del
OAC de la Delegació del Govern a Lleida
Propietat Forestal, Centre de la
Torelló-Torelló Jove, Ajuntament de
Ajuntament de Castelldefels
Calonge, Ajuntament de
Centre Municipal d'Informació Juvenil
Oficina Municipal d'Atenció Ciutadana
Ajuntament de Santa Coloma de Gramenet
Ajuntament de Gurb
Ajuntament de Montblanc
Ajuntament de Vidreres
Ajuntament de Quart
Ajuntament de Palau-saverdera
Ajuntament de Tossa de Mar
Ajuntament Vilanova del Camí
Ajuntament de Vilafranca del Penedès
Ajuntament de Sitges
Ajuntament de Sitges
Ajuntament de Sitges
Ajuntament de Sant Andreu de Llavaneres
Ajuntament del Papiol
Ajuntament d'Olivella
Ajuntament de Sitges
Ajuntament de Sabadell. SAC Est
Ajuntament de Sabadell. SAC Oest
Ajuntament de Monistrol de Montserrat
Ajuntament de Sant Pere de Vilamajor
Ajuntament de Subirats
Ajuntament de Tremp
Ajuntament de Torelló
Ajuntament de Gavà

Ajuntament de l'Ametlla de Mar
Ajuntament de Lloret de Mar - El Puntet
Ajuntament del Pla de Santa Maria
Montsià, Consell Comarcal del
Universitat Pompeu Fabra
Universitat Pompeu Fabra
Universitat Pompeu Fabra
BASE. Oficina Altafulla
BASE. Oficina Amposta
BASE. Oficina Calafell
BASE. Oficina Creixell
BASE. Oficina de Cunit
BASE. Oficina de Deltebre
BASE. Oficina del Vendrell
BASE. Oficina Falset
BASE. Oficina Gandesa
BASE. Oficina Hospitalet de l'Infant i Vandellòs
BASE. Oficina La Canonja
BASE. Oficina La Sénia
BASE. Oficina Miami platja
BASE. Oficina Montblanc
BASE. Oficina Mont-roig del Camp
BASE. Oficina Móra d'Ebre
BASE. Oficina Reus
BASE. Oficina Riudoms
BASE. Oficina Roda de Berà
BASE. Oficina Sant Carles de la Ràpita
BASE. Oficina Torredembarra
BASE. Oficina Tortosa
BASE. Oficina Ulldecona
BASE. Oficina Valls
BASE. Oficina Vila-seca
Ajuntament de Lloret de Mar - Biblioteca Municipal de Lloret
Institut Municipal d'Informàtica
Ajuntament de Sant Esteve Sesrovires
Ajuntament de Figueres
Ajuntament de Celrà
Ajuntament de Reus
Ajuntament de Salou
Ajuntament d'Arenys de Mar
Ajuntament de Sant Quirze del Vallès
Ajuntament de les Preses
Ajuntament de Bigues i Riells
Ajuntament de Sant Llorenç Savall
Ajuntament de Vilobí d'Onyar
Consell Comarcal de les Garrigues

Ajuntament de Sant Feliu de Llobregat
Ajuntament d'Olot

Ajuntament d'Aitona

Ajuntament de Balaguer
Ajuntament de Bell-lloc d'Urgell
Ajuntament de Cerdanyola del Vallès
Ajuntament de l'Escala
Ajuntament de Pineda de Mar
Ajuntament d'Hostalric
Consell Comarcal de la Garrotxa
Consell Comarcal de la Segarra
Consell Comarcal de l'Alta Ribagorça
Consell Comarcal del Berguedà
Priorat, Consell Comarcal del
Ajuntament de Gelida
Ajuntament de Vilanova i la Geltrú
Ajuntament de Llinars del Vallès

UAB - Campus de Sabadell

Ajuntament de Sant Llorenç d'Hortons
Ajuntament de Centelles
Fundació Universitària Balmes. Universitat de Vic-UCC
OAIC - Centre Cívic Onyar
OAIC - Centre Cívic Pla de Palau
OAIC - Centre Cívic Pont Major
OAIC - Centre Cívic Sant Narcís
OAIC - Centre Cívic Santa Eugènia
OAIC - Llar d'avis de Taialà
OAIC - Plaça del Vi, 1
Ajuntament de Cornellà de Llobregat
Ajuntament de Salt
Ajuntament d'Esparreguera
Ajuntament de l'Hospitalet de Llobregat
Ajuntament de Calafell
Consell Comarcal del Ripollès
Ajuntament de Sabadell. SAC Nord
Ajuntament de Sabadell. SAC Sud
Consell Comarcal del Pla d'Urgell
Ajuntament de Dosrius
Ajuntament de Calaf
Ajuntament de Corbera de Llobregat
Oficina d'Atenció Ciutadana (OAC) dels Serveis Territorials d'Empresa i Treball a Tarragona

Oficina d'Atenció Ciutadana (OAC) d'Empresa i Treball

Departament de Cultura - ST Girona Casa Solterra
Departament de Cultura - ST Lleida
Departament de Cultura- ST Catalunya Central
Departament de Cultura- ST Terres de l'Ebre

Departament de Cultura - ST Tarragona
Oficina d'Atenció Ciutadana (OAC) dels Serveis Territorials d'Empresa i Treball a Lleida
Ajuntament de Sant Martí de tous
Ajuntament de Calella
Ajuntament de les Masies de Voltregà
Ajuntament d'Arbúcies
Ajuntament de Castellterçol
Ajuntament de Fogars de la Selva
Ajuntament de la Garriga
Ajuntament de Massanes
Ajuntament de Sant Andreu de la Barca
Ajuntament de Teià
Ajuntament de Torroella de Montgrí
BASE. Oficina Alcanar
Conselh Generau d'Aran
Consell Comarcal de la Cerdanya
Consell Comarcal de l'Alt Urgell
Consell Comarcal del Baix Penedès
Ajuntament de Polinyà
Ajuntament de Palamós
Consell Comarcal del Segrià
Ajuntament de Sant Feliu de Guíxols
BASE. Oficina Tarragona
Consell Comarcal de la Noguera
Consell Comarcal d'Osona
Institut Municipal d'Ocupació
Oficina de Gestió i Atenció Tributària
Ajuntament de Cubelles
Ajuntament de Terrassa - Oficina d'Atenció Ciutadana de Plaça Didó - OAC1
Ajuntament de Terrassa - Oficina d'Atenció Ciutadana del Districte 2 - OAC2
Ajuntament de Terrassa - Oficina d'Atenció Ciutadana del Districte 3 - OAC3
Ajuntament de Terrassa - Oficina d'Atenció Ciutadana del Districte 4 - OAC4
Ajuntament de Terrassa - Oficina d'Atenció Ciutadana del Districte 5 - OAC5
Ajuntament de Terrassa - Oficina d'Atenció Ciutadana del Districte 6 - OAC6
Ajuntament de Terrassa - Oficina d'Atenció Ciutadana del Districte 7 - OAC7
Ajuntament de Vilassar de Dalt
Ajuntament de Lloret de Mar
Ajuntament de Mollet del Vallès
Ajuntament de Moià
Ajuntament de Sant Joan de les Abadesses
Consell Comarcal del Pallars Sobirà
Ajuntament de Molins de Rei
OAC de la Generalitat de Catalunya a Barcelona

Ajuntament de Canet de Mar
Ajuntament de Canyelles
Ajuntament de Collbató
Ajuntament de Palau-solità i Plegamans
Ajuntament de Santa Eulàlia de Ronçana
Ajuntament de Sentmenat
Ajuntament de Mediona
Ajuntament de Sant Pol de Mar

Taxi, Institut Metropolità del
Ajuntament de Tàrrega

Punt d'informació del Departament de Territori
Ajuntament d'Esplugues de Llobregat
Ajuntament de Ripollet
Ajuntament de Masquefa - CTC - MASQUEFA
Consell Comarcal de l'Alt Camp
Ajuntament d'Òdena
Ajuntament de Sant Vicenç dels Horts. SIAC
Oficina d'Atenció Ciutadana a Tarragona
Oficina d'Atenció Ciutadana del Departament de Treball Afers Socials i Famílies a les Terres de l'Ebre
Oficina d'Atenció Ciutadana del Departament de Treball Afers Socials i Famílies a Lleida
Consell Comarcal de la Terra Alta
Ajuntament de Breda
Departament d'Acció Exterior i Unió Europea
Ajuntament d'Almacelles
Consell Comarcal del Baix Camp
Ajuntament de Berga
Ajuntament de Tordera
Ajuntament de Torelló - La Carrera
Ajuntament de Granollers
Ajuntament de Carme
Ajuntament del Morell
Ajuntament de Viladasens
Ajuntament de Castellfollit de la Roca
Ajuntament de Prats de Lluçanès
Ajuntament de Blanes
Ajuntament de Palafrugell
Ajuntament de Sant Pere de Ribes
Ajuntament de Sant Pere de Ribes
Ajuntament de Rubí-RAMBLETA
Ajuntament del Masnou
Ajuntament de Caldes de Montbui
Ajuntament de l'Ametlla del Vallès
Ajuntament de Lliçà d'Amunt

Ajuntament de Lliçà de Vall
Ajuntament de Llagostera
Ajuntament de Riudellots de la Selva
Consell Comarcal de la Ribera d'Ebre
Ajuntament d'Alcanar
Consell Comarcal del Solsonès
Ajuntament de Viladecavalls
Ajuntament de Castellbisbal
Sant Sadurní d'Anoia, Ajuntament de
Ajuntament de la Llagosta
Ajuntament de Navàs
Ajuntament de Sant Joan Despí
Ajuntament d'Olesa de Montserrat
Ajuntament de Montornès del Vallès
Consell Comarcal de l'Alt Penedès

Ajuntament de Torelló - La Cooperativa

Oficina d'Afers Socials i Famílies de Barcelona - Sants / Eixample
Ajuntament de Vic - ER idCAT de la Biblioteca
Ajuntament de Vic - ER idCAT de la Plaça Major

Ajuntament del Vendrell

Ajuntament de Sant Hilari Sacalm
Ajuntament d'Albatàrrec
Ajuntament de Castellolí
Ajuntament de Parets del Vallès
OAC SAV
Ajuntament de Cabrils
Ajuntament de Santpedor
Ajuntament de Cardedeu
Ajuntament de Guissona

Ajuntament de Malgrat de Mar

Ajuntament de Polinyà - Centre de Serveis a l'Empresa i l'Emprenedoria
Ajuntament de Polinyà - El Roure
Ajuntament de Santa Perpètua de Mogoda
Ajuntament de Vilassar de Mar
Consell Comarcal de l'Urgell
Consell Comarcal del Maresme
Ajuntament de Montcada i Reixac
Ajuntament de Valls
Ajuntament de Castellet i la Gornal
Ajuntament de Sant Feliu de Buixalleu
Ajuntament de Premià de Dalt
Oficina d'Atenció Ciutadana del Districte Administratiu
Ajuntament de Santa Bàrbara
Ajuntament del Prat de Llobregat
OAC Aragó - Departament de Territori

OAC Casa Gasset (Tarragona)- Departament de Territori
OAC Clot de les Monges (Lleida)
Ajuntament de Viladecans
Ajuntament de Santa Cristina d'Aro
Ajuntament de Matadepera
Ajuntament de la Torre de Claramunt
Ajuntament de Camprodon
Ajuntament de Mont-roig del Camp
Ajuntament de Salomó
Ajuntament de Cambrils
Ajuntament d'Argentona
Ajuntament de Constantí

L'Aleixar, Ajuntament de

Ajuntament dels Hostalets de Pierola
Ajuntament de Sant Feliu de Codines
Consell Comarcal del Tarragonès
Ajuntament d'Arenys de Munt
Delegació Territorial del Govern a les Terres de l'Ebre
Universitat de Barcelona
Ajuntament de Campllong
Ajuntament de Rubí-Narcís Menard
Ajuntament d'Alella
Ajuntament de Montmeló
Ajuntament de Roses
Ajuntament de les Franqueses del Vallès
Ajuntament de Riells i Viabrea
Consell Comarcal de la Selva
Consell Comarcal del Baix Empordà
Ajuntament de les Borges del Camp
OAC de la Generalitat de Catalunya a Tarragona
Ajuntament de La Bisbal del Penedès
Ajuntament de Badia del Vallès
Ajuntament de Mieres
Consell Comarcal de l'Anoia
Ajuntament de Premià de Mar
Ajuntament de Brunyola i Sant Martí Sapresa
Ajuntament de Manresa
Ajuntament de Sant Hipòlit de Voltregà
Ajuntament de Castellar del Vallès
Ajuntament de Sant Boi de Llobregat
Ajuntament de la Tallada d'Empordà
Consell Comarcal de la Conca de Barberà
Ajuntament de Canet d'Adri
Ajuntament d'Anglès

Delegació del Govern de la Generalitat de Catalunya a Mèxic i a l'Amèrica Central
Delegació del Govern de la Generalitat de Catalunya a Alemanya
Delegació del Govern de la Generalitat al Con Sud
Consell Comarcal del Baix Llobregat
Consell Comarcal del Vallés Oriental
Ajuntament dels Alamús
OAC de la Delegació Territorial del Govern a Girona
Baix Ebre, Consell Comarcal del
Oficina d'Atenció Ciutadana del Departament de Treball Afers Socials i Famílies
Ajuntament de Martorell
Ajuntament de Sant Vicenç de Castellet
Oficina d'Atenció Ciutadana de Barcelona

Ajuntament de la Llacuna

OAC de la Delegacio de Govern de Tarragona
Oficina d'Atenció Ciutadana de la Cerdanya
Treball, Afers Socials i Famílies - OAC Albareda, Departament de

(*) aquest llistat es a data juny 2024 i pot variar al llarg del temps.

Ens titular de l'ER T-CAT	núm ER's	impressió pin des de la LRA	recuperació de pin des de la carpeta del subscriptor	Tipus Targeta	Disseny del plàstic	grabació amb lector extern (no impressora de targetes)	aprovador + generador	Altres personalitzacions
Badalona, Ajuntament de	1	opcionalment	SI	pròpia	T-CAT BADALONA	SI	NO	No aplica
Castelldefels, Ajuntament de	1	opcionalment	SI	T-CAT	T-CAT ESTANDARD	NO	NO	No aplica
Cornellà de Llobregat, Ajuntament de	1	opcionalment	SI	T-CAT	T-CAT ESTANDARD	NO	NO	No aplica
Manresa, Ajuntament	1	opcionalment	SI	T-CAT	T-CAT ESTANDARD	NO	NO	No aplica
Mataró, Ajuntament de	1	opcionalment	SI	T-CAT	T-CAT ESTANDARD	NO	NO	No aplica
Mollet del Vallès, Ajuntament	1	opcionalment	SI	pròpia	T-CAT Mollet	SI	NO	No aplica
Sabadell, Ajuntament de	1	opcionalment	SI	pròpia	no aplica	SI	NO	No aplica
Sant Feliu de Llobregat, Ajuntament	1	opcionalment	SI	T-CAT	T-CAT ESTANDARD	NO	NO	No aplica
Cerdanyola del Vallès. Ajuntament de	1	opcionalment	SI	T-CAT	T-CAT ESTANDARD	NO	NO	No aplica
Politècnica de Catalunya, Universitat	17+1	opcionalment	SI	bancària	no aplica	SI	SI	No aplica
Pompeu Fabra, Universitat	8	opcionalment	SI	bancària	no aplica	SI	SI	No aplica
Lleida, Universitat de	2	opcionalment	SI	bancària	no aplica	SI	SI	No aplica
Universitat Rovira i Virgili	25	opcionalment	SI	bancària	no aplica	SI	SI	No aplica
Girona, Ajuntament de	1	opcionalment	SI	T-CAT	T-CAT ESTANDARD	NO	SI	No aplica
Barcelona, Universitat de	25	opcionalment	SI	bancària	no aplica	SI	SI	No aplica
Lleida, Ajuntament de	1	opcionalment	SI	pròpia	no aplica	SI	NO	No aplica
Reus, Ajuntament	1	opcionalment	SI	pròpia	T-CAT FOTO	NO	NO	No aplica
Tarragona, Ajuntament	1	opcionalment	SI	pròpia	T-CAT ESTANDARD	NO	NO	No aplica
CTTI	1	opcionalment	SI	pròpia	no aplica	SI	NO	No aplica
Catalana de la Protecció de Dades, Agència	1	opcionalment	SI	T-CAT	T-CAT ESTANDARD	NO	NO	No aplica
Parlament	1	opcionalment	SI	pròpia	T-CAT PARLAMENT	NO	NO	No aplica
ORGT de la DIBA	1	opcionalment	SI	pròpia	T-CAT ORGT	NO	NO	No aplica
Tarragona, Diputació de	1	opcionalment	SI	pròpia	T-CAT ESTANDARD	NO	NO	No aplica
Alt Camp, Consell Comarcal de l'	1	opcionalment	SI	T-CAT	T-CAT ESTANDARD	NO	NO	No aplica
Alt Empordà, Consell Comarcal	1	opcionalment	SI	T-CAT	T-CAT ESTANDARD	NO	NO	No aplica
Alt Penedès, Consell Comarcal del	1	opcionalment	SI	T-CAT	T-CAT ESTANDARD	NO	NO	No aplica
Alt Urgell, Consell Comarcal del	1	opcionalment	SI	T-CAT	T-CAT ESTANDARD	NO	NO	No aplica
Alta Ribagorça, Consell Comarcal de l'	1	opcionalment	SI	T-CAT	T-CAT ESTANDARD	NO	NO	No aplica
Anoia, Consell Comarcal de l'	1	opcionalment	SI	T-CAT	T-CAT ESTANDARD	NO	NO	No aplica
Bages, Consell Comarcal del	1	opcionalment	SI	T-CAT	T-CAT ESTANDARD	NO	NO	No aplica
Baix Camp, Consell Comarcal del	1	opcionalment	SI	T-CAT	T-CAT ESTANDARD	NO	NO	No aplica
Baix Ebre, Consell Comarcal del	1	opcionalment	SI	T-CAT	T-CAT ESTANDARD	NO	NO	No aplica
Baix Empordà, Consell Comarcal del	1	opcionalment	SI	T-CAT	T-CAT ESTANDARD	NO	NO	No aplica
Baix Llobregat, Consell Comarcal del	1	opcionalment	SI	T-CAT	T-CAT ESTANDARD	NO	NO	No aplica
Baix Penedès, Consell Comarcal del	1	opcionalment	SI	T-CAT	T-CAT ESTANDARD	NO	NO	No aplica
Berguedà, Consell Comarcal del	1	opcionalment	SI	T-CAT	T-CAT ESTANDARD	NO	NO	No aplica
Cerdanya, Consell Comarcal de la	1	opcionalment	SI	T-CAT	T-CAT ESTANDARD	NO	NO	No aplica
Conca de Barberà, Consell Comarcal de la	1	opcionalment	SI	T-CAT	T-CAT ESTANDARD	NO	NO	No aplica
Garraf, Consell Comarcal del	1	opcionalment	SI	T-CAT	T-CAT ESTANDARD	NO	NO	No aplica
Garrigues, Consell Comarcal de les	1	opcionalment	SI	T-CAT	T-CAT ESTANDARD	NO	NO	No aplica
Garrotxa, Consell Comarcal de la	1	opcionalment	SI	T-CAT	T-CAT ESTANDARD	NO	NO	No aplica
Gironès, Consell Comarcal del	1	opcionalment	SI	T-CAT	T-CAT ESTANDARD	NO	NO	No aplica
Maresme, Consell Comarcal	1	opcionalment	SI	T-CAT	T-CAT ESTANDARD	NO	NO	No aplica
Montsià, Consell Comarcal del	1	opcionalment	SI	T-CAT	T-CAT ESTANDARD	NO	NO	No aplica
Noguera, Consell Comarcal de la	1	opcionalment	SI	T-CAT	T-CAT ESTANDARD	NO	NO	No aplica
Osona, Consell Comarcal d'	1	opcionalment	SI	T-CAT	T-CAT ESTANDARD	NO	NO	No aplica
Pallars Jussà, Consell Comarcal del	1	opcionalment	SI	T-CAT	T-CAT ESTANDARD	NO	NO	No aplica
Pallars Sobirà, Consell Comarcal del	1	opcionalment	SI	T-CAT	T-CAT ESTANDARD	NO	NO	No aplica
Pla de l'Urgell, Consell Comarcal del	1	opcionalment	SI	T-CAT	T-CAT ESTANDARD	NO	NO	No aplica
Pla de l'Estany, Consell Comarcal del	1	opcionalment	SI	T-CAT	T-CAT ESTANDARD	NO	NO	No aplica
Priorat, Consell Comarcal	1	opcionalment	SI	T-CAT	T-CAT ESTANDARD	NO	NO	No aplica

Ribera d'Ebre, Consell Comarcal de la	1	opcionalment	SI	T-CAT	T-CAT ESTANDARD	NO	NO	No aplica
Ripollès, Consell Comarcal del	1	opcionalment	SI	T-CAT	T-CAT ESTANDARD	NO	NO	No aplica
Segarra, Consell Comarcal de la	1	opcionalment	SI	T-CAT	T-CAT ESTANDARD	NO	NO	No aplica
Segrià, Consell Comarcal del	1	opcionalment	SI	T-CAT	T-CAT ESTANDARD	NO	NO	No aplica
Selva, Consell Comarcal de la	1	opcionalment	SI	T-CAT	T-CAT ESTANDARD	NO	NO	No aplica
Solsonès, Consell Comarcal del	1	opcionalment	SI	T-CAT	T-CAT ESTANDARD	NO	NO	No aplica
Tarragonès, Consell Comarcal del	1	opcionalment	SI	T-CAT	T-CAT ESTANDARD	NO	NO	No aplica
Terra Alta, Consell Comarcal de la	1	opcionalment	SI	T-CAT	T-CAT ESTANDARD	NO	NO	No aplica
Urgell, Consell Comarcal de l'	1	opcionalment	SI	T-CAT	T-CAT ESTANDARD	NO	NO	No aplica
Aran, Conselh Generau d'Aran	1	opcionalment	SI	T-CAT	T-CAT ESTANDARD	NO	NO	No aplica
Moianès, Consell Comarcal del	1	opcionalment	SI	T-CAT	T-CAT ESTANDARD	NO	NO	No aplica
Vallès Occidental, Consell Comarcal del	1	opcionalment	SI	T-CAT	T-CAT ESTANDARD	NO	NO	No aplica
Valles Oriental, Consell Comarcal del	1	opcionalment	SI	T-CAT	T-CAT ESTANDARD	NO	NO	No aplica
AOC	2	opcionalment	SI	T-CAT	tots	NO	NO	No aplica
CESICAT	1	opcionalment	SI	pròpia	no aplica	SI	NO	No aplica

Consorci
Administració Oberta
de Catalunya

Descripció funcional de la plataforma SCD

Generalitat de Catalunya

LOCALRET

Realitzat per: AOC
Versió: 1.3
Data: 9/7/2024
Arxiu: Descripcio_plataforma_SCD.docx

Index

1 Definicions i acrònims

1.1 Definicions

DISPOSITIU: Suport on es graven els certificats emesos, per exemple, una targeta criptogràfica específica, un fitxer PKCS#12 en un directori, o una memòria USB. El sistema ha d'utilitzar els diferents dispositius físics via interfície PKCS#11.

ENS. Organisme amb usuaris que necessiten i utilitzen els certificats emesos. Normalment serà el valor del camp O del certificat. Està lligat a un codi d'ens que és la base per els filtres de visibilitat de dades que utilitza el sistema a partir del rol de cada operador.

ENTITAT DE REGISTRE. Oficina on hi ha operadors del sistema. Una Entitat de Registre pot peticionar o veure certificats d'un o varis ens sobre els que està autoritzat. Al mateix temps, pot tramitar certificats d'una o vàries Entitats de Certificació i d'un o varis perfils de certificat de cada Entitat de Certificació. Cada Entitat de certificació té un tipus especial d'Entitat de Registre (codi 000) que pot tractar certificats de qualsevol ens.

LOT. Conjunt de peticions de certificació agrupades sota un mateix identificador i que permet realitzar operacions globals per tots els seu elements.

OPERADOR. Persona o programari, identificat mitjançant un certificat digital, que pot accedir al sistema del SCD i realitzar les funcions definides per el seus rols.

PERFIL DE CERTIFICAT. Certificat o conjunt de certificats que emet el sistema. En la definició del perfil es podran especificar coses com: certificats a emetre (per exemple firma i xifrat), dades necessàries per el certificat, dades de gestió (adreces, etc), dades per la personalització gràfica del suport (fotografia, disseny, etc.), regles d'unicitat que apliquen als certificats, etc.
En cas que un perfil generi més d'un certificat, el sistema permetrà realitzar les operacions del cicle de vida (revocació, suspensió, consulta, etc) de manera conjunta i transparent des del punt de vista dels operadors.
El sistema disposa de diferents Entitats de Certificació que al mateix temps emeten diferents perfils cadascuna. Dins el concepte perfil Cada perfil es pot generar sobre un o varis dispositius diferents.

POSSEÏDOR DE CLAUS. Usuari titular del certificat i que serà el responsable del seu ús.

RESPONSABLE DE SERVEI. És l' interlocutor i gestor principal davant del servei per un ens.

ROL. Propietat associada a un Operador i que defineix les operacions que pot fer. Un operador pot tenir més d'un rol , sempre que aquests no siguin incompatibles.

SISTEMA ONLINE. Part del sistema del SCD que permet generar certificats de manera completa a partir de les dades de la petició.

SISTEMA LOTS. Part del sistema del SCD que permet generar els fitxers a partir de l'enviament d'informació en forma de Lot al fabricant de targetes, En aquest esquema les tasques logístiques queden repartides entre el fabricant de targetes i la AOC. Aquest sistema només es aplicable a un conjunt reduït de certificats i perfils, sempre en suport targeta criptogràfica.

1.2 Acrònims

CRL. Llista de certificats revocats (Certificate Revocation List)

EC. Entitat de Certificació

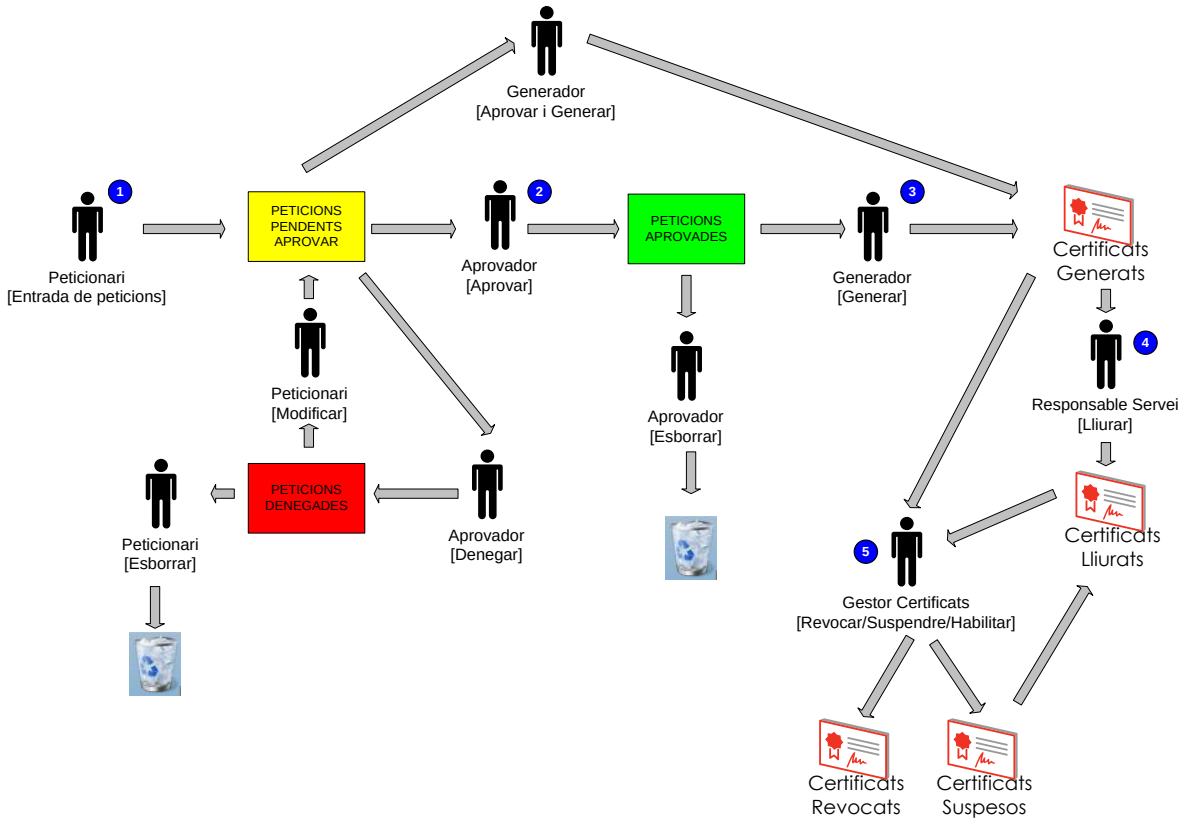
ER. Entitat de Registre

ERV. Entitat de Registre Virtual

SCD. Servei de Certificació Digital

2 Descripció general del processos de certificació.

Per entendre el funcionament del sistema, a continuació és detalla quin és el flux de la informació dins del SCD. La següent figura mostra aquest flux en funció del seu ordre cronològic més natural dins el sistema ONLINE. A continuació es descriuen cadascun dels passos i una breu descripció dels processos més importants associats a cadascun d'ells.



Dins el sistema poden existir algunes excepcions al flux general mostrat en funció de requeriments addicionals que poden aplicar a un perfil de certificat , a una Entitat de certificació o a una Entitat de registre.

2.1 Fase 1. Introducció de peticions.

En aquests pas es realitza la 'gravació' de les dades de la petició de certificació dins la base de dades del SCD. Aquesta acció es pot realitzar de diferents maneres en funció de si el certificat serà generat pel sistema ONLINE o per el sistema de LOTS. Aquest dos entorns tenen petites diferències de funcionament.

Sistema ONLINE

Durant aquest procés es realitzen les operacions de validació de les dades (longitud, DNI, valors limitats per llistes, etc) i les validacions d'unicitat. Si la petició s'introdueix correctament al sistema , aquesta queda en estat PENDENT.

També existeix un estat esborrany que permet a l'operador tenir les peticions en *esborrany* i que només són visibles només per ell mateix.

Destacar que el valor del camp ens (normalment traslladat al camp O del certificat) està limitat per la llista d'ens associats a la ER que opera el peticionari.

Sistema LOTS

Quan s'introdueixen les diferents peticions, es realitzen les operacions de validació de les dades (longitud, DNI, valors limitats per llistes, etc). En aquest punt les peticions les podríem considerar que estan en estat DRAFT ja que només son visibles per el propi operador.
És en el moment que s'executa l'acció de TANCAR LOT, que és verifica la unicitat i les peticions (englobades dins el LOT) queden en estat PENDENT D'APROVAR.

2.2 Fase 2. Aprovació de peticions.

En aquest fase, es permet als operadors, APROVAR o DENEGAR les peticions. Com en el cas anterior, hi ha petites diferències entre el sistema ONLINE i el sistema de LOTS.

Sistema ONLINE

Es permeten les operacions d'APROVAR, DENEGAR i ESBORRAR per cadascuna de les peticions que estan en estat PENDENT D'APROVAR. Cal realitzar la una signatura digital per cada petició que quedarà registrada al sistema.

Sistema LOTS

És permeten les operacions de APROVAR i DENEGAR a nivell del LOT que s'ha creat en el pas anterior. Cal realitzar una signatura digital per cada lot que quedarà registrada al sistema.

2.3 Fase 3. Generació

En aquesta fase és el moment en que es generen els certificats. Com en el casos anteriors hi ha diferències entre el sistema ONLINE i el sistema de LOTS:

Sistema ONLINE

Mitjançant KeyOne LRA, es recuperen les peticions pendents de generar i el sistema gestiona els elements necessaris per la seva generació en el corresponent suport (targetes, impressores, lectors, etc.). En aquest pas es genera la documentació relacionada a cada certificats:

- Full de lliurament
- Sobre cec, amb PIN i PUK, per els perfils en targeta i en format certificat o PKCS #12 per la resta de perfils. Aquest element es continua generant però la seva impressió ja no és realitza. L'enviament el fa el sistema per correu electrònic un cop lliurat el certificat.

També realitza la publicació del full de lliurament i dels codis PIN i PUK al servidor de la RA per tal de poder fer l'enviament de manera automàtica.

Sistema LOTS

Mitjançant KeyOne LRA, es recuperen els lots aprovats pendents de generar i el sistema genera els fitxers que cal enviar al servei extern de generació de targetes. Una vegada fet aquest flux, queda sota la responsabilitat del generador de les targetes de generar la documentació associada i la logística del seu lliurament.

Aquesta operativa només està disponible en els entorn KeyOne LRA ubicats dins la AOC.

2.4 Fase 4. Lliurament

Una vegada generats els certificats aquest han de ser lliurats als seus destinataris.

En la operativa inicial del servei SCD (fins al 2009) aquesta fase era 'externa' al servei del SCD i constava de les següents operacions:

- Enviament de les targetes al responsable del servei o dels certificats/PKCS#12 per correu de manera manual.
- Enviament dels fulls de lliurament al responsable del servei.
- Enviament del sobres de PIN i PUK al posseïdor de les claus.
- Recepció de la còpia del full de lliurament, degudament signada per el posseïdor de claus, per part de la AOC i tancament de l'expedient associat al gestor documental.

A partir del 2009 i per minimitzar l'ús del paper en els anteriors passos, es defineix el flux de la següent manera:

- Enviament de les targetes al responsable del servei. En el cas dels certificats/PKCS#12 el propi responsable del servei podrà realitzar la descàrrega dels mateixos a través del portal del servei SCD.
- El Responsable del Servei rep les targetes, accedeix a la web del SCD amb el seu certificat i realitza les següents operacions:

- Marca a la web del SCD que ha rebut els certificats. [Aquesta operació comporta la realització d'una signatura digital]
- Descarrega els fulls de lliurament
- Lliura les targetes o els PKCS#12/certificats (prèvia descàrrega dels fitxers) i fa signar el full de lliurament al posseïdor de les claus i els custodia. Marca a la web del SCD que ha lliurat els certificats. [Aquesta operació comporta la realització d'una signatura digital]
- El sistema, una vegada detecta que els certificats han estat lliurats, envia el PIN/PUK (o paraula de pas del PKCS#12) per correu electrònic signat al posseïdor de les claus, indicat a la petició. Serà responsabilitat de l'ens si s'utilitza una mateixa adreça per diferents peticions.

2.5 Fase 5. Cicle de vida

A part del cicle de generació descrit en els passos anteriors. El sistema permet la gestió de l'estat dels certificats.
A través del portal del SCD, per els rols 'Gestors' podran realitzar el canvi d'estat dels certificats associats a la seva ER.

Aquestes operacions comporten també la realització d'una signatura digital que quedarà registrada al sistema.

3 Rols del sistema

A continuació és detallen cadascun dels rols dels sistema SCD i que estan lligats a les operacions que podran realitzar i en quina fase del flux definit en el capítol anterior.

La gestió dels operadors i el seu rols es realitza per part d'un Administrador a partir dels certificats CIPISR o CDA, excepte en els casos indicats expressament.

3.1 Peticionari

Rol d'operador encarregat d'entrar les sol·licituds de certificats.
També podrà importar fitxers en format text que permet la introducció massiva de peticions. Aquesta opció és pot definir per cada operador.

Opcions Menú

- Introduir peticions
- Cercar peticions

Permisos especials

- Pot importar peticions en fitxer

Tipus de certificats vàlids per ser utilitzats per aquest rol

- CIPISR emesos per diverses ECs.
- CDAs emesos per diverses ECs. Aquest són per les aplicacions que fan servir el connector i, per tant, tindran activat el permís per tal d'importar peticions a nivell de fitxer.

3.2 Peticionari Lots

Rol d'operador encarregat de la gestió de lots de peticions per a ser enviades a un proveïdor extern. Es tracta d'un rol reservat a personal de la AOC. Tots els filtres i el control d'unicitat de les peticions s'executen en aquesta fase.

Opcions Menú

- Nou Lot
- Gestionar Lots
- Gestionar plantilles

Tipus de certificats vàlids per ser utilitzats per aquest rol

- CIPISR emesos per diverses ECs.

3.3 Aprovador

Rol d'operador encarregat d'aprovar les sol·licituds existents i de deixar-les disponibles per a generar el certificat.

Opcions Menú

- Cercar peticions

Tipus de certificats vàlids per ser utilitzats per aquest rol

- CIPISR emesos per diverses ECs.

3.4 Aprovador Lots

Rol d'operador encarregat de l'aprovació dels lots dels lots generats pel peticionari de lots.
Es tracta d'un rol reservat a personal de la AOC.
En cas de denegació, podrà indicar les peticions amb errors i consignar comentaris addicionals.

Opcions Menú

- Gestionar Lots

Tipus de certificats vàlids per ser utilitzats per aquest rol

- CIPISR emesos per diverses ECs.

3.5 Generador

Rol d'operador encarregat de generar els certificats a partir de sol·licituds prèviament aprovades.
Es podrà activar la possibilitat de realitzar les operacions d'aprovació i generació de manera unitària.

Tipus de certificats vàlids per ser utilitzats per aquest rol

- CIPISR emesos per diverses ECs.

Addicionalment a la gestió feta des del portal del SCD, aquest operadors cal gestionar-los en una segona capa dins l'entorn de KeyOne CA, definint-los com a Registration Officer.

3.6 Generador Lots

Rol d'operador encarregat de generar la informació per l'enviament a un proveïdor a partir dels lots prèviament aprovats.

Tipus de certificats vàlids per ser utilitzats per aquest rol

- CIPISR emesos per diverses ECs.

Addicionalment a la gestió feta des del portal del SCD, aquest operadors cal gestionar-los en una segona capa dins l'entorn de KeyOne CA, definint-los com a Registration Officer.

3.7 Gestor Certificats

Rol d'operador encarregat d'efectuar diferents operacions corresponents al cicle de vida dels certificats existents (suspendre, habilitar i revocar).

Opcions Menú

- Cerca

- Cerca avançada

Permisos especials

- Operacions permeses. Revocar, suspendre, habilitar
- Revocació automàtica. (Revocació a través d'un connector)

Tipus de certificats vàlids per ser utilitzats per aquest rol

- CIPISR emesos per diverses ECs.

3.8 Responsable del servei de l'Entitat de Registre T-CAT

Operador al càrrec d'una i només una Entitat de Registre que té privilegis per veure l'estat de les peticions de la ER i obtenir informes d'activitat de la mateixa.

Opcions Menú

- Estat peticions
- Informes

Tipus de certificats vàlids per ser utilitzats per aquest rol

- CIPISR emesos per diverses ECs.

3.9 Responsable del servei de l'Entitat de Registre Virtual

Usuari interlocutor i gestor principal de cada ens davant del servei. Serà encarregat de la fase de lliurament i també podrà obtenir informes d'activitat del seu ens. Algú pot ser responsable de més d'un ens

Opcions Menú

- Informes de servei
- Gestió de Lliurament i PINs
- Seguiment de les peticions pròpies (estat de tramitació)

Tipus de certificats vàlids per ser utilitzats per aquest rol

- Certificats personals, normalment CPISR

Gestió dels operadors

En aquest cas la gestió, i degut al gran nombre de potencials operadors és realitza de manera externa al sistema. El servei del SCD és, per tant, autogestionat gràcies a les consultes fetes al sistema de mestre d'ens, ja disponible dins els sistemes de la AOC. El sistema realitza una replicació periòdica automàtica.

Les dades disponibles del Mestre d'ens són:

- Descripció de l'ens
- Dades del responsable de servei (i dels corresponents suplents)

- Nom i cognoms
- Correu electrònic
- DNI del responsable

L'algoritme de decisió durant l'autenticació de l'operador serà el següent:

A.- Obtenir el certificat CPISR utilitzat en la connexió SSL
B.- Obtenció del DNI contingut dins el certificat CPISR
C.- Obtenció de la llista d'ens habilitats per el DNI obtingut

3.10 Administrador

Operador amb màxims privilegis, entre ells el de crear altres operadors i concedir-los els permisos adequats, i mantenir els fitxers mestres d'Entitats de Registre, ens, perfils i dispositius. Restringit a operadors de la AOC.

Opcions Menú

- Operadors
- Entitat de Registre
- Llista d'ens
- Gestió lliurament
- Gestió DNS

Tipus de certificats vàlids per ser utilitzats per aquest rol

- CIPISR emesos per diverses ECs.

Gestió dels operadors

Aquests operadors es basen en un llista de confiança (ACL signada digitalment) configurada a l'eina i gestionada per l'Àrea Tècnica. Cal comunicar els **números de sèrie dels certificats** a l'Àrea Tècnica perquè la pugui configurar.

3.11 Dipositari AOC

Operador amb permisos per efectuar el lliurament i la descàrrega de certificats cedits per els ens a la AOC.

Opcions Menú

- Cerca/Descàrrega

Tipus de certificats vàlids per ser utilitzats per aquest rol

- CIPISR emesos per diverses ECs.

3.12 Compatibilitat entre rols

A continuació es mostra una taula indicant els rols que són compatibles per un mateix operador:

	Peticionari	Peticionari Lots	Aprovador	Aprovador Lots	Generador	Generador Lots	Gestor Certificats	Responsable del servei de l' Entitat de Registre	Responsable del servei de l' Entitat de Registre Virtual	Administrador
Peticionari on line		SI	NO	NO	SI	SI	SI	SI	NO	SI
Peticionari Lots			NO	NO	SI	SI	SI	SI	NO	SI
Aprovador on line				SI	SI*/No	SI*/NO	SI	SI	NO	SI
Aprovador Lots					SI*/No	SI*/No	SI	SI	NO	SI
Generador on line						SI	SI	SI	NO	SI
Generador Lots							SI	SI	NO	SI
Gestor Certificats								SI	NO	SI
Responsable del servei de l'Entitat de Registre									NO	SI
Responsable del servei de l'Entitat de Registre Virtual										SI
Administrador										

*** Sí, només en cas que hagin fusionat aprovador+generador.**

4 Mòduls funcionals de la infraestructura

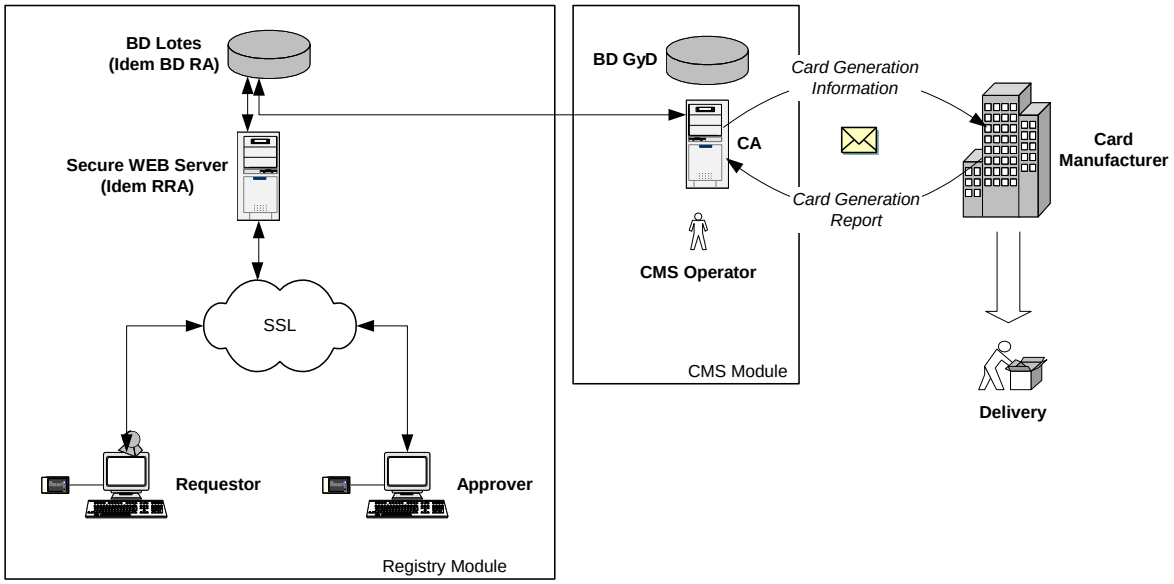
A continuació es descriu amb més detall diferents mòduls del sistema. Aquests aporten funcionalitats que apliquen a parts del flux descrit en capítols anteriors i també operacions enumerades en la definició dels rols del sistema.

Aquesta descripció mes detallada ha de permetre tenir una visió més exacte de la seva funció, funcionalitat i per tan impacte sobre el sistema global.

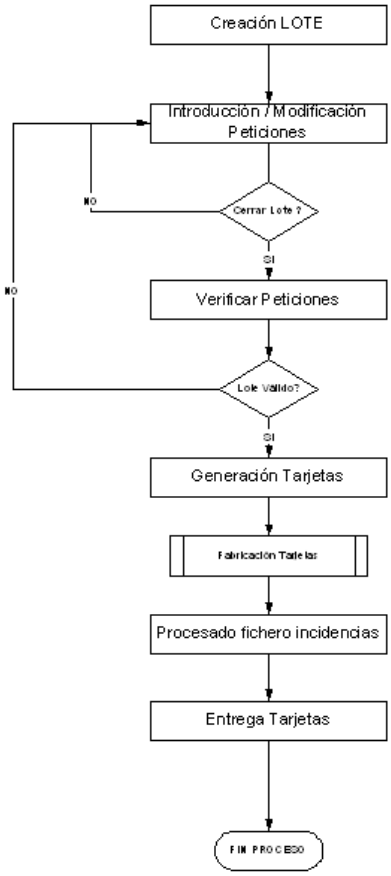
4.1 Sistema d'emissió per lots

Aquest mòdul permet la gestió de les peticions i agrupacions d'aquestes (LOTS) que permeten la generació de les targetes de manera massiva i directa a les instal·lacions de GyD.

L'arquitectura d'aquesta part dins el sistema de certificació està descrita la següent figura.



A continuació és mostra el flux de les dades en aquest circuit de certificació.



Com es pot observar en les anterior figures, a part de la interfície WEB per la introducció i aprovació de dades cal una peça per la gestió del cicle entre la AOC i GyD, CMS Module. Aquest mòdul està implementat amb KeyOne LRA , que permet realitzar les operacions a partir de les dades i que interaccionen tan amb la fàbrica de targetes (GyD) com amb l'entitat de certificació (KeyOne CA).

Les operacions per cada fase del procés , identificades també amb el seu rol són:

Rol Peticionari

- → Creació/gestió de lots de peticions
- → Introducció de les dades de les peticions de manera
  - → Manual
  - → Importació de fitxer
  - → Recuperació de peticions amb incidències
  - → Importació a partir de la base de dades del sistema ONLINE
- → Exportació de peticions cap al sistema ONLINE
- → Creació/gestió de lots de plantilles de dades
- → Visualització de les peticions una vegada emès el lot

Rol Aprovador

→ Visualització/aprovació/denegació de lots de peticions
→ Canvi d'estat d'un lot en procés de producció.

Rol Generador (KeyOne LRA)

→ Generació del fitxer .req amb les dades de les targetes a generar
→ Tractament del fitxer .ret amb les claus públiques, generació dels certificats i generació del fitxer .batch que ja conté els certificats i els PKCS#12 de xifrat.
→ Tractament del fitxer d'incidències .inc que tanca el cicle amb el fabricant de les targetes.

A continuació es detallen altres aspectes a tenir en compte d'aquest mòdul.

4.1.1 Accés al sistema

Per accedir al mòdul cal disposar de:

- Certificat d'operador reconegut amb rol PETICIONARI o APROVADOR
- Connexió al servidor WEB intern (Important: mòdul no disponible des de les oficines de la AOC)
- Navegador Internet Explorer + FormSign X (part aprovador)
- Només disponible actualment per les entitats EC-AL i EC_SAFP

4.1.2 Estats dels lots

A continuació és descriuen els diferents estats que pot tenir un lot.

Codi Estat	***Estat***	***Descripció***	**Qui pot operar-lo*?***
100	Obert	Lot creat i disponible per la modificació i introducció de peticions	PETICIONARI
200	Tancat	Lot preparat per la seva aprovació	APROVADOR
300	Aprovat	Lot preparat per la seva generació a partir de la LRA	GENERADOR o APROVADOR
400	Emès	Lot en procés de fabricació	GENERADOR o APROVADOR
500	Rebut	Lot finalitzat. Es pot procedir al lliurament de les targetes.	PETICIONARI (lectura)

4.1.3 Estats de les peticions.

A continuació és descriuen els diferents estats que pot tenir una petició dins un lot. Aquest estat canvi de manera automàtica en realitzar algun pas del flux del sistema.

Codi Estat Estat Descripció

0	VALID	Petició introduïda per el peticionari. És marca com a vàlida però no assegura que contingui les dades necessàries.
1	VERIFIED	Petició verificada por l'aprovador
2	INVALID	Petició invalidada per l'aprovador
3	ISSUED	Petició correcta pendent de lliurament de la targeta
4	DELIVERED	Petició correcta i lliurada al posseïdor
5	ERROR	Petició que ha causat error durant la fabricació de la targeta
6	RE-ISSUED	Petició que ha causat error y posteriorment s'ha recuperat per la seva reemissió.

4.1.4 Rol Peticionari

4.1.4.1 Funcionalitat generals

- Cada peticionari gestiona els seus lots i plantilles de lots, per tan els peticionaris no comparteixen en cap cas la informació continguda en el lot. El sistema actual, no permet doncs, que un peticionari pugui veure lots d'un altre peticionari sigui quin sigui l'estat del mateix.
- Totes les operacions és realitzen a nivell de lot i per tan el primer que te que fer el peticionari és accedir/crear un lot.
- Només és poden introduir les peticions que estan suportades dins el sistema de lots. Actualment tenim les següents polítiques:

EC-AL
- CPISR-1
- CESR-1
- CPISRC-1

EC-SAFP
- CPISR-1
- CPISR-1-J
- CESR-1
- CPISRC-1

4.1.4.2 Plantilles de lot

- Les plantilles de lot defineixen un conjunt de dades prefixades que s'utilitzaran per defecte si durant la introducció /importació de la petició aquestes no estan definides.
- Es permeten les operacions de ALTA, MODIFICACIÓ i BAIXA de les plantilles.
- Les plantilles es visualitzen a partir de la dada introduïda en el camp **NOM**.
- Les plantilles son exclusives de cada usuari.

4.1.4.3 Gestió manual de peticions

- El formulari de visualització de dades és fix per tots els tipus de certificat
- En l'operació d'alta s'omplen els camps amb el valor de la plantilla relacionada al lot
- És realitzen validacions de les dades a nivell de Javascript en determinats camps
- Si falta una dada obligatòria cal omplir-la per seguir endavant
- Al visualitzar una petició la podrem MODIFICAR o ESBORRAR

4.1.4.4 Importació de peticions a partir del sistema ONLINE

- El cercador de peticions contra el sistema de certificació ONLINE amb el mateix 'look' que tenen els cercadors dels aprovadors actuals, incloent el ID_TRAMESA
- Si s'importa una petició en estat aprovat, la informació d'aquesta aprovació (signatura) és perd
- El mòdul que permet importar les peticions del mòdul ONLINE al mòdul de lots és el Mòdul Peticionari del sistema de LOTS.
- Per fer la importació el sistema permet cercar peticions en qualsevol estat, és a dir pendents d'aprovar, aprovades i denegades
- Una petició importada al sistema de lots desapareix del sistema ONLINE per sempre (cal per temes d'unicitat)
- La funció d'importació executa la mateixa validació de dades que s'aplica actualment a la importació de dades a partir de fitxer pla.

- En el cas de les peticions CPISR_1_J cal tenir en compte que la fotografia que es troba al sistema ONLINe no es trasllada al sistema de LOTS.

4.1.4.5 Importació de peticions a partir de fitxer

- És mante la possibilitat d'importar peticions a partir del fitxer generat amb ACCES (sortida_lot.txt)
- El format d'aquest fitxer està definit al document ***'Format d'importació peticions per sistema LOTS_v1.4.doc'*** situat al directori M:\NouPrometeo\Departaments\Tecnica\Documentacio_PKI_CATCERT\LOTS\
- El sistema d'importació té en compte els valors de la plantilla associada per els camps no definits al fitxer
- És realitzen una sèrie de validacions abans d'acceptar cada registre

4.1.4.6 Recuperació de peticions errònies

- El sistema permet importar també peticions errònies d'altres lots en estat REBUT.
- Al realitzar aquesta operació la petició origen queda en estat Re-issued
- Aquesta operació afecta a tots els lots en estat rebut

4.1.4.7 Exportació de peticions al sistema ONLINE

- Quan visualitzem la llista de peticions d'un lot és permet l'exportació de les mateixes
- L'exportació insereix al sistema ONLINE la petició amb les dades de peticionari del operador que està operant
- Les peticions queden per defecte en estat pendent d'aprovar
- En el cas de les peticions CPISR_1_J cal tenir en compte que
    - S'importa en estat DRAFT

- La fotografia queda sense informar

Tancament del LOT

- El peticionari 'ordena' la generació d'un lot a partir del seu tancament
- En l'operació de tancament és verifica la unicitat de les peticions introduïdes tan contra la taula certificats com el sistema ONLINE.
- És valida que dins el lot no existeixin dues peticions amb el mateix DNI. Aquesta restricció està originada per el procediment de generació que utilitza GyD.

4.1.5 Rol Aprovador

- És poden visualitzar els lots en estat TANCAT i EMES
- Per defecte és visualitzen el lots dels darrers 3 mesos
- Sobre el lots en estat tancat poden Aprovar o refusar el Lot
- A nivell de petició podem assignar una raó de denegació per cada petició
- L'aprovació implica la realització d'una signatura digital amb FormSign
- Les dades signades son un resum de les peticions del lot
- Sobre un lot en estat emès podem tornar-lo a estat OBERT. Aquesta operació nomes és per casos excepcionals d'error durant la generació del fitxer .ret amb la LRA de Lots

4.2 Gestió de dissenys/personalitzacions de targetes

Aquest mòdul permet la gestió dels diferents tipus de targeta física i que poden contenir en el seu xip certificats de polítiques diferents.
Així, per exemple, un certificat de tipus CPISR-1 podrà generar-se en diferents tipus de plàstic en funció de l'ens final on estaran destinades.
També és pot gestionar a nivell de permisos de l'operador quins dissenys de targetes pot generar una determinada **Entitat de registre**

4.2.1 Requeriments

A continuació s'enumeren una llista de requeriments que suporta el nou mòdul

- Sistema per gestionar de manera més eficient els possibles dissenys de targetes diferents presents a la plataforma de certificació.
- Sobre un mateixa política de certificat (per exemple CPISR) poden aplicar N dissenys de targeta
- El disseny és escollit per part del peticionari a partir d'un desplegable en el moment d'introduir les dades de la petició
- Els dissenys disponibles per una política serà la intersecció entre **els dissenys lligats al perfil** i **els disseny permesos ala ER del peticionari (entitat de registre associada).** Per exemple si el CPISR-1 té com a perfils la següent llista:
    - D1. Targeta CATCert
    - D2. Targeta Justicia amb FOTO
    - D3. Targeta Justicia sense FOTO

I es connecta un operador amb codi d'entitat de registre determinat (per exemple 300, justícia) que només pot generar els dissenys D2 i D3, el desplegable de dissenys només contindrà els valors D2 i D3.

- Des del mòdul d'administració es configuren els dissenys lligats a cada ER

4.2.2 Solució tècnica i funcionament

A continuació és descriu la solució tècnica que s'ha implementat per assolir els requeriments descrits.
Aquesta aproximació a la implementació permet entendre d'una manera més clara els passos que cal fer en el moment que és vol afegir o modificar les dades lligades a un determinat disseny.

4.2.3 Fitxers de mapeig i disseny

Cada disseny està format per dos fitxers de definició :

1. **Fitxer de disseny físic (per exemple FIS_CATCERT_3L.ws)**. Conté les característiques físiques del disseny tals com:
    a. Número i posició de les línies d'impressió que van tan al anvers com el revers.
    b. Mida de la lletra de cada línia
    c. Alineació de les línies
    d. Posició de les imatges o logos
    e. Presencia de dades la banda magnètica
2. **Fitxer de mapeig de dades**. Principalment conté tota la lògica necessària per 'lligar' les dades del formulari amb les línies físiques definides en el fitxer de disseny físic. Dins aquest fitxer es poden:

    a. Incloure nous camps que apareixeran al formulari i que ens permetran demanar a l'operador dades que només es fan servir per imprimir, per exemple una fotografia.
    b. Fixar el lligam entre dades del formulari i el disseny físic poden incorporar, per exemple, parts fixes de text.
    c. Opcionalment es poden tornar a definir camps del formulari que ja estan definits a nivell del fitxer de política per fer-los mes restrictius (per exemple és limita el camp de l'organització a un desplegable de 1 sol valor)

4.2.4 Fitxer <policy>.ws

Dins aquest fitxer es defineixen les següents dades:

1. Dades relatives al certificats i dades de gestió.
2. Apareix un camp dins el fitxer de política, **card_design**, i que es defineix del tipus llista amb un conjunt de valors igual a la llista de DISSENYS disponibles per aquesta política. Per exemple per CPISR_1 de SAFP tenim
    spec_card_design <<<! spec_EOF

label = Tipus de targeta
type = INFO
values =
MAP_CATCERT_BASIC,MAP_JUSTICIA_BASIC,MAP_CAC_BASIC
default_selected = MAP_CATCERT_BASIC
filter_variable = op_design_list
spec_EOF

Amb aquestes definicions s'aconsegueix poder reaprofitar el mateix fitxer de política tot i que aquest es pugui generar en targetes tan diferents com la de per defecte o la de JUSTICIA.

4.2.5 Configuració a l'entitat de registre. WEB Administració

Dins el perfil de l'er es pot:

1. Configurar per cada entitat de registre el conjunt de dissenys que pot generar de la llista de dissenys disponibles i definits a config_admin_miscoptions.ws
2. Els operadors tindran lligada la seva configuració a la seva entitat de registre a la que pertanyen.

4.2.6 Funcionament

Quan un operador (peticionari) és connecta al servei:

→ s'obté de la seu perfil la llista de dissenys permesos per la seva entitat de registre.
→ al seleccionar una política es fa la intersecció entre la llista de dissenys de l'operador i la llista de dissenys de la política. Si el resultat és >1 apareix un desplegable per seleccionar el tipus de targeta. Si el resultat és 1 es passa automàticament al següent pas.
→ És genera el formulari a partir de les dades del fitxer de política més les dades addicionals definides dins el fitxer de mapeig.

4.2.7 Passos per incorporar un nou disseny

De manera resumida, la incorporació d'un nou disseny comporta els següents passos:

1. Crear el fitxer de definició físic
2. Crear el fitxer de mapeig
3. Modificar els fitxer de polítiques que aplica el nou disseny
4. Modificar el fitxer de template_definitions.ws per incorporar el nou disseny
5. Modificar el fitxer de configuració de la part d'administració
6. Entrar a nivell d'administració i activar el nou perfil a les entitats de registre corresponents.

4.3 Sincronització de la llista d'ens

Cada operador que accedeix al sistema SCD, a part de determinades excepcions, no podrà veure, per exemple, tots els certificats de l'EC. El sistema filtrarà els ens en funció del perfil de l'operador. Aquest filtres de dades tenen efectes pràctics sobretot en dos punt del flux:

Petició de certificats. El filtre limitarà el conjunt de valors vàlids en el camp **Organització** dels formularis. No és permetrà la introducció de valors lliures per el camp organització.

Gestió de certificats. El filtre limitarà el conjunt de certificats que podrà veure l'operador i, per tant, gestionar-ne el seu estat.
El sistema realitzarà la següent seqüència per establir a quins ens pot accedir l'operador.

1. Obtenir l'ER a la que pertany l'operador
    - Accedir a les propietats de l'ER i obtenir la llista de d'ens associats
2. Aplicar als filtres de cerca la llista obtinguda en el punt anterior

L'anterior seqüència no s'aplica als següents rols que tenen una visió global de totes les peticions:

- Peticionari Lots
- Aprovador Lots
- Generador Lots

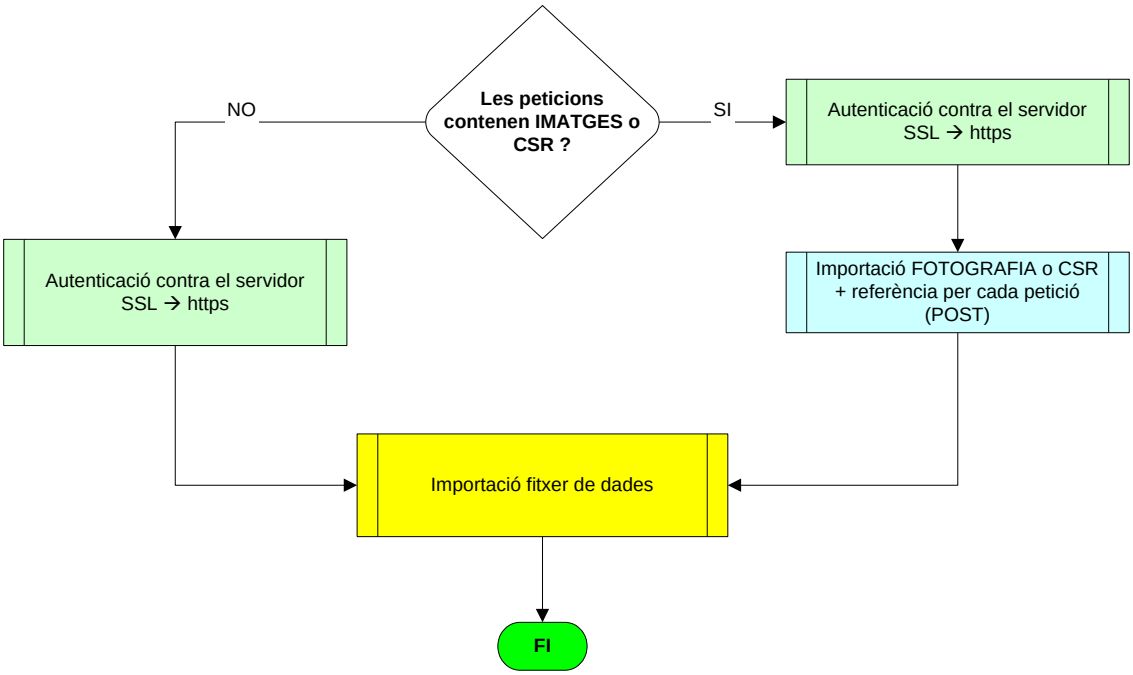
Tampoc s'aplica a tots els operadors de **la ER amb codi 000.**

El rol **Responsable del servei de l'Entitat de Registre Virtual** té un comportament **especial** ja que només podrà veure les peticions o certificats associats al seu ens.

El sistema genera la taula d'ens dins la seva base de dades a partir d'una sincronització entre l'entorn PKI i l'entorn on està el mestre de tercers.

Aquesta sincronització es realitza mitjançant una tasca programada en l'entorn de la màquina de gestió de la PKI amb les següents característiques:

- S'executa cada 30 minuts
- Actualitza les dades dels ens i també dels responsables titulars i suplents associats a cadascun d'ells.
- Una vegada finalitzada la sincronització esborra els registres que ja no han estat sincronitzats (és tracta d'una baixa).
- En cada execució genera traces i informes en format CSV amb les següents elements:
    - Ens amb descripció massa llarga i que per tan no són vàlids per la generació de certificats (actualment fixat a 57 caràcters)
    - Llista de certificats orfes de la BD de la CA. Són aquells que tenen associat un CODI_ENS que no existeix al mestre. Aquests certificats només poden ser operats per operador associats a la ER amb codi 000.
    - Per defecte els ens nous s'associen a la ER 000
    - Els ens es poden separar per EC en funció d'un camp del sistema de Tercers.



4.4 Interfícies per operacions automàtiques

4.4.1 Introducció de dades

El procés d'entrada d'una petició a la plataforma de certificació pot dur-se a terme per mitjà d'un operador (persona humana) de l'entitat de certificació o per mitjà d'un procés automàtic (una màquina/programa). A continuació es descriu el mòdul que permet la recepció peticions automàtiques.

Tècnicament es tracta d'un CGI disponible dins del portal del servei SCD (https amb autenticació de client). Per realitzar una petició el client requereix disposar d'un certificat d'aplicació (**CDA**).
La petició serà un *POST* de les dades de la petició seguint un format determinat. En funció del tipus de certificat que es vulgui peticionar el nombre de camps requerits i el format de les dades variarà.
Si la petició conté algun camp de dades que pot ser de mida gran, per exemple fotografies i/o peticions de certificat (CSR) s'haurà de realitzar la importació en dues passes. La primera consistirà en la importació de la fotografia o CSR juntament amb un referència i el segon pas importa la resta de dades de la petició.
A continuació es mostra una figura amb el flux de la importació d'una petició.

Per una altra banda el client pot sol·licitar tres accions diferents associades a una petició:

- **ALTA**: permet entrar un petició nova dintre de la plataforma.

- **MODIFICACIÓ**: permet canviar alguna de les dades associades amb alguna petició ja existent. El camp que es fa servir per identificar la petició és el document d'identificació (NIF, NIE, etc.) juntament amb el tipus del certificat de la petició.
- **BAIXA**: permet eliminar alguna petició ja existent en la plataforma. El camp que es fa servir per identificar la petició és el document d'identificació (NIF, NIE, etc.) juntament amb el tipus del certificat de la petició.

A part de les operacions, el mòdul té dos maneres de funcionar

- En mode **Normal**.
- En mode **Transacció**.

A continuació és descriuen de manera funcional els dos modes.

Importació de peticions en mode NORMAL

En aquest mode les peticions son introduïdes de manera unitària al sistema i no comporten la realització de tasques addicionals a les definides en el procediment general.
Així en un fitxer amb diferents peticions, el resultat de la importació pot ser satisfactori per alguns dels registres i errònia per una altra part.
Per altra banda en aquest cas no es farà us d'alguns dels camps del fitxer d'importació lligats a la importació en mode transacció. Aquests paràmetres son:

- ID_TRAMESA - identificador de tramesa
- CODI_ENS - Codi de l'ens

Importació de peticions en mode TRANSACCIÓ

En aquest mode les peticions son introduïdes de manera conjunta (transaccional) al sistema i **comporten la realització de tasques addicionals** a les definides en el procediment general.
Així en un fitxer amb diferents peticions, si el resultat de la importació d'un registre és erroni, cap de les peticions serà importada dins el sistema.
En aquest mode i de manera addicional al procediment estàndard d'importació definit anteriorment, és realitzen les següents accions.

1. Si la importació és correcte es crea un registre dins la taula de **TRAMESES**
2. Es tracten les noves dades ID_TRAMESA i CODI_ENS.
3. El valida que el valor de ID_TRAMESA és igual en tot el fitxer
4. També és genera de forma automàtica la dada POS_TRAMESA com la posició de la petició dins la tramesa (calculada automàticament de 1 a N)

4.4.2 Integració del mòdul

URLs de servei

En funció de l'entitat de certificació per la qual es vulgui carregar una petició s'haurà de fer servir un url o una altra. Actualment, els serveis de registre automàtic que estan operatius per les següents Ecs i en les següents urls:
https://scd.catcert.cat/connectors/connector.ws?idCA=<valor>

On idCA pot tenir els següents valors:

- EC_AL

- EC_SAFP
- EC_UR
- EC_URV
- EC_PARLAMENT

Si volem realitzar la importació en mode transacció caldrà afegir a les anteriors URLs **&importMode=TRANS.**

Per la importació d'objectes del tipus fotografia o CSR caldrà utilitzar la mateixa URL, és a dir:

https://scd.catcert.cat/connectors/connector.ws?idCA=<valor>

Serà en funció d'altres paràmetres enviats a aquesta URL que el sistema realitzarà una operació o una altra.

Notar que des del mòdul peticionari de cada EC també es permet la importació dels fitxers de text que contenen les peticions.

Per accedir a aquesta URL caldrà una targeta d'operador habilitada al sistema, amb rol Peticionari i el permís específic per importar peticions.

Passos integració

L'aplicació tindrà que fer un post a l'adreça indicada en el punt anterior amb les següents variables:

- **importPet.** Ha de contenir el fitxer de text en el format definit i coherent amb el següent paràmetre.
- **operationType.** Pot tenir dos valors:
  - **ENROLL_DATA.** Per operacions d'introducció de peticions. En aquest cas importPet ha de ser aquest format 0
  - **ENROLL_OBJ.** Per operacions d'introducció de fotografies o CSRs. En aquest cas importPet ha de ser aquest format 0

Per fer aquest post caldrà establir **una connexió SSL amb el servidor** i **autenticar-se amb el certificat CDA** proporcionat.

Urls de proves

Per tal de poder provar si el desenvolupament de la part client funciona disposem de URLs en l'entorn de preproducció.
Per fer les proves caldrà disposar d'un certificat d'aplicació de l'entorn de preproducció (CDA) per el servidor preproduccio.catcert.net. Per obtenir-lo contactar amb la AOC a desenvolupament@catcert.net.
Les URLs de preproducció son les mateixes de producció canviant https://scd.catcert.cat per www.preproduccio.catcert.net.

4.4.3 Format general dels fitxers d'importació

En els següents apartats es mostra el format i camps que han de contenir les peticions de manera general per tots els tipus de certificats. A partir d'aquestes pautes generals caldrà 'acabar' de generar el fitxer en funció del tipus de certificat que volem peticionar. La

documentació associada a cada tipus de certificat es pot obtenir directament del sistema (veure Obtenir fitxers d'exemple per cada tipus de certificat).

Format pel fitxer d'importació de fotografies o peticions de certificació CSR

El format del fitxer d'importació de dades tipus Petició de certificació (CSR) o fotografies és el següent:

Línia 1, Valor fix

```
IDENTIFICADOR|VALOR
```

Línies de peticions

```
<REFERENCIA>|<VALOR>
```

On

→ **REFERENCIA** és el un identificador alfanumèric lliure de longitud màxima 10.

→ **VALOR** és la petició de certificació o la fotografia en format textual **BASE64 sense salts de línia**.

IMPORTANT. Encara que el valor d'origen ja estigui en base64, SEMPRE cal aplicar la transformació del valor a base64 sense salts de línia

Exemple

```
IDENTIFICADOR|VALOR
00A123ASER|TUlJQ0R6Q0NBWGlnQXdJQkFnSUJBRE.....EVWa2IrSmZkWDBSUk5vRHEvMExSNUNnMlQ4
```

Format pel fitxer d'importació de peticions

El format del fitxer d'importació de peticions és **autodefinit,** és a dir en el primer registre defineix els camps que incorpora la petició. Així el format del fitxer serà el següent:

Línia 1

DEFINICIO|OPERACIO|ESTAT|OPERADOR|ID_TRAMESA|CODI_ENS|<Llista de camps separats per |>

Línies de peticions

<ID_POLITICA>|<OPERACIÓ>|<ESTAT>|<OPERADOR>|<ID_TRAMESA>|<CODI_ENS><<Valors>

On

→ **Llista de camps** és el la llista de camps de la petició. Aquesta llista depèn del tipus de certificat. La pròpia aplicació permetrà la generació i descàrrega de fitxers d'exemple per cada tipus de política que tingui permesa l'operador.

→ **ID_POLITICA** és el codi que identifica la política. Per exemple CPISR_1, CESR_1, CDS_1, etc.

→ **OPERACIO** és la operació que volem realitzar sobre la petició. Els valors possibles son

- **ALTA**. Nova petició
- **MOD**. Modificació de peticions. En cas de no existir es comporta igual que l'operació ALTA
- **BAIXA**. Esborrar petició

→ **ESTAT** és l'estat en que quedarà la petició dins la base de dades. Els valors possibles son:

- **PENDENT**. Peticions en estat Pendent d'aprovar
- **APROVADA**. Peticions en estat aprovat.
- **ESBORRANY**. Peticions en estat esborrany

→ **OPERADOR** és el codi d'operador que s'inserirà a la base de dades. Aquest valor permet gestionar el flux de les peticions dins el sistema de registre de l'entitat de certificació (codis de ER) serà la AOC qui donarà la els codis en funció de la naturalesa de l'aplicació d'importació de peticions. El codi del OPERADOR es fixa tan al camp **codipeticionari** com **codiaprovador** al realitzar importacions amb el codi especificat dins el fitxer.
→ **ID_TRAMESA. [OPCIONAL]** És el codi de la tramesa. El seu format és de l'estil 3bc3755b-1101-4ccf-b3a8-8955bccpf690
→ **CODI_ENS. [OPCIONAL]** És el codi de l'ens. El seu format és de l'estil 800600000.

Exemple

```
DEFINICIO|OPERACIO|ESTAT|OPERADOR|cn|cn2|doc_type|doc_num|ea|user_upn|categoria|carre
c|ou|o|cif_org|resp_nom|resp_nif|resp_ea|resp_address|resp_cp|resp_pob|foto
CPISR_1|ALTA|PENDENT|0001001|Josep|Català
Pujol|NIF/NIE|91554344B|estu1234@urv.es|w2000@domini|TU -Titulars
d'universitat|càrrec|departament|URV|11223344E|Josep Morei
Gualta|98786545Q|jmorei@urv.es|c/ passeig l'oreneta, 25|43001|Tarragona|ref_foto
```

Com podem veure en l'exemple anterior el valor de la columna foto és el valor de la referència utilitzada en el pas anterior.

4.4.4 Obtenir fitxers d'exemple per cada tipus de certificat

El sistema permet obtenir la llista de camps d'un tipus de certificat així com un fitxer d'exemple per la importació d'una petició cal seguir els següents passos:

1. Accedir amb un certificat d'operador o el propi certificat CDA a la URL del servei
2. El sistema té una opció per accedir a una pàgina amb la llista dels tipus de certificats disponibles per l'operador.
3. En aquest moment es generen fitxers d'exemple per cada combinació de política i disseny de targeta disponible, permetent la descàrrega del mateix.

4.4.5 Interpretació dels missatges de sortida:

Es retorna informació sobre l'estat de finalització de la càrrega de cada petició del fitxer d'entrada. S'identifica cada petició d'entrada amb el número de línia que ocupava en el fitxer d'entrada acompanyat d'un missatge d'estat de finalització que pot ser "OK" o "ERROR". En el caso d'"ERROR", acompanya un petit text descriptiu de l'error i, en alguns casos, es mostra el valor que ha originat el missatge d'error.
Les peticions amb indicador d'estat de finalització "**OK**" hauran estat carregades correctament dins el sistema. Junt amb l'identificador OK, apareix un ID, és tracta de l'identificador única de la petició dins la base de dades ENROLL. Les aplicacions no ha de fer ús d'aquest ID.
Les peticions amb indicador d'estat de finalització "**ERROR**" no hauran estat carregades en el sistema ja que no complien alguna de les restriccions de format dels camps o del fitxer requerides per aquell perfil. El missatge que acompanyarà aquest indicador aportarà informació respecte de l'origen de l'error.

Exemple de sortida

1.ERROR|El codi de pais del passaport/DNI forani no és vàlid (AA). Consulti la llista de codis de pais vàlids.
2. OK|A13423BEF67
3.ERROR|El camp Passaport/DNI forani no pot ser nul
4.ERROR|El camp Passaport/DNI forani = ES-1234567895665465465465465465409876543210987654321 supera la longitud màxima 15
5.ERROR|Format de Passaport/DNI forani incorrecte (ES11SFA54321).
6.ERROR|El codi de pais del passaport/DNI forani no és vàlid (AA). Consulti la llista de codis de pais vàlids.
7. OK|F1323EA90A
8.ERROR|El camp Passaport/DNI forani = ES-123456789546546546540987654321098765432 1 supera la longitud màxima 15
9.ERROR|El camp Passaport/DNI forani no pot ser nul
10.ERROR|Format de Passaport/DNI forani incorrecte (ES11SFA54321).

4.4.6 Revocació de certificats

Els requeriments del mòdul de revocació automàtica són:

- Possibilitat de revocar certificats de a partir d'una crida automàtica al sistema, sense necessitat de operar la consulta avançada
- El procés remot s'autenticarà al sistema mitjançant l'ús del protocol SSL i presentant un certificat del tipus CDA
- El certificat CDA estarà habilitat al sistema de consulta avançada amb rol Gestor i activant l'opció de 'Revocació automàtica'.
- Els certificats que sobre els que podrà operar un CDA en concret estaran limitats als ens que tingui relacionat aquest certificat, a partir de la ER assignada.
- Les operacions de canvi d'estat des de la WEB deixen una traça signada de l'operació dins el sistema. En el cas del connector, aquesta traça serà signada per el certificat intern.
- Existeix un mode de funcionament, orientat a l'ús des de EACAT, que permet realitzar les operacions de forma TRANSACCIONAL. Només es realitza la operació si tots els registres del fitxer d'entrada son correctes.
- L'ús del mode TRANSACCIONAL comporta la creació automàtica d'un registre de TRAMESA dins el sistema. Aquest fet no té cap implicació directe sobre les operacions de revocació.
- Es podrà indicar en la petició si es volen revocar també els certificats relacionats al indicat. És considera un certificat relacionat el que
    - té el mateix codi de suspensió
    - està emès en un temps proper
- El registre de la taula de trameses conté les següents dades
    → Número de tramesa - > generat aleatòriament
    → Data de recepció i finalització coincideixen
    → Dades del operador. S'obtenen del CDA que envia el fitxer a la consulta avançada
    → Tipus TRAMESA codi **200**

4.4.6.1 Funcionament

El flux del mòdul de revocació és el següent:

→ Obtenir dades del certificat SSL (CDA)
→ Consultar el ROL del certificat al sistema. Te que ser Administrador o Revocació automàtica'
→ Carregar el fitxer de peticions amb nom revocationFile
→ Per cada línia del fitxer
→ Verificar que no es tracta d'un número de sèrie repetit dins el fitxer
→ Verificació del codi de raó existeix a la configuració
→ Verificar l'existència del número de sèrie. (aquí s'aplica el filtre de ER si procedeix) i si està indicat en el paràmetre corresponent obtenir els certificats relacionats.
→ Verificar que el certificat (i els relacionats) no està caducat
→ Verificar que l'acció requerida no sigui incompatible amb l'estat actual del certificat
→ Realitzar les operacions de revocació en un sol lot de revocació i generar la traça signada.
→ Generar sortida

4.4.6.2 Integració amb el mòdul

URLs de serveis i requeriments

La URL del mòdul de revocació en el seu mode de funcionament **NORMAL** serà:
https://scd.catcert.cat/connectors/connector.ws?idCA=<valor>

On idCA pot tenir els següents valors:

- EC_AL
- EC_SAFP
- EC_UR
- EC_URV
- EC_PARLAMENT

La URL del mòdul de revocació en el seu mode de funcionament **TRANSACCIONAL** serà:
https://scd.catcert.cat/connectors/connector.ws?idCA=<valor>&importMode=TRANS

On idCA pot tenir els següents valors:

- EC_AL
- EC_SAFP
- EC_UR

L'aplicació que accedeixi disposarà d'un certificat de tipus CDA i les corresponents claus per la seva verificació i també per verificar el certificat del servidor https://scd.catcert.cat.

Passos integració

L'aplicació tindrà que fer un post a l'adreça indicada en el punt anterior amb les següents variables:

- **revocationFile.** Ha de contenir el fitxer de text de les peticions de revocació.
- **operationType.** Valor fix a **REVOKE**

Per fer aquest post caldrà establir **una connexió SSL amb el servidor** i **autenticar-se amb el certificat CDA** proporcionat.

Format del fitxer de peticions

El fitxer de text que conté les peticions tindrà el següent format:
Línia 1
SERIAL|ACCIO|RAO|MODE|CIF
Línies de peticions
NUMERO_DE_SERIE|OPERACIO|RAÓ|MODE|CIF

On
→ **NUMERO_DE_SERIE**. Número de sèrie del certificat, sense espais i en majúscules
→ **OPERACIO**. Operació a realitzar sobre el certificats. Les operacions possibles son **REVOCAR**, **SUSPENDRE** o **HABILITAR**.
→ **RAÓ.** Raó associada a l'acció. Veure per les possibles combinacions.
→ **MODE.** Indica si es vol actuar sobre els certificats relacionats o no. Hi ha dos valors possibles:
000 – Aplica només al certificat indicat
001 – Aplica al certificat indicat i els seus relacionats si existeixen
→ **CIF.** Valor del CIF de l'ens del certificat.
El fitxer podrà contenir **N registres amb números de sèrie diferents**.

Exemple

SERIAL|ACCIO|RAO|MODE|CIF
44918ADC7106693643B409DEDB1ED9BF|SUSPENDRE|S01|001|A12345678
7AAEBD0D2D5DE71843B409DE61FA71FC|REVOCAR|R01|001|A12245678
761E3D8A562C6A2F437DDEA9302C75EA|REVOCAR|R02|000|A12343278
18C410A5F42376CC43B415F2C304AF4C|HABILITAR|H01|001|A11115678

Format del fitxer de resposta

La resposta de l'operació POST, retorna una pàgina text/html que contindrà un registres per cadascun del registres del fitxer d'entrada amb el següent format.

NUMERO_REGISTRE|RESULTAT|CODI_ERROR|DESCRIPCIO_ERROR

On
→ **NUMERO_REGISTRE**. Número de registre relacionat amb el fitxer d'entrada. Comença per 0.
→ **RESULTAT**. Resultat de l'operació. Les resultats possibles son **OK** o **ERROR**.
→ **CODI_ERROR.** Codi d'error produït. Veure per les possibles combinacions.
→ **DESCRIPCIÓ_ERROR.** Descripció de l'error.

Exemple

0|ERROR|E12|El certificat amb número de sèrie
44918ADC7106693643B409DEDB1ED9BF no existeix
1|OK|
2|OK|
3|ERROR|E15|

4.4.6.3 Relació de raons de revocació i referència d'errors

Raons de Revocació
La següent taula conté les diferents raons de revocació en funció de l'operació requerida.

ACCIÓ	CODI RAÓ	Descripció
HABILITAR	**H01**	Habilitar certificat
SUSPENDRE	**S01**	Sospita de que el certificat conté dades incorrectes
	S02	Sospita de pèrdua del dispositiu criptogràfic o del certificat
	S03	Sospita d'ús o accés a la clau privada del certificat per part d'un tercer
	S99	Altres
REVOCAR	**R01**	Compromís de la informació continguda en el certificat
	R02	Compromís de la seguretat de la clau o del certificat
	R03	Compromís del dispositiu criptogràfic
	R04	Motius referents al subscriptor o al posseïdor de claus
	R99	Altres

4.4.6.4 Relació d'errors

La següent taula resumeix els possibles errors que es poden produir al utilitzar el mòdul de revocació automàtica.

CODI_ERROR	Descripció
ERRORS GENERALS	
E00	Error inesperat del sistema. La descripció proporciona l'error de baix nivell.
E01	Certificat CDA no disposa de permisos per utilitzar el servei
ERRORS PER REGISTRE	
E10	El número de sèrie està repetit dins el fitxer
E11	Error al realitzar la consulta del número de sèrie dins la BD La descripció proporciona l'error de baix nivell.
E12	El certificat especificat no existeix, o l'usuari no te permisos sobre ell, o el CIF* indicat no és correcte
E13	El certificat especificat està caducat. No es pot realitzar cap operació sobre ell.
E14	El certificat especificat és vàlid i per tan no es pot habilitar.
E15	El certificat especificat està suspès i per tan no es pot suspendre
E16	El certificat especificat està revocat. No es pot realitzar cap operació sobre ell.
E17	La raó especificada no està definida
E18	La raó i l'acció no son coherents

***Nota**: Les validacions sobre el valor del CIF no estan actives actualment.

4.5 Sincronització d'operadors

Per tal de tenir una capa més de seguretat, el sistema permet la definició de les relacions entre operadors amb rol aprovador i operadors amb rol generador.

Quan un aprovador i un generador estan relacionat significa que el generador podrà processar i per tan generar el certificats de les peticions aprovades per el rol aprovador.

Aquesta relació és defineix en el portal SCD per part dels operadors Administradors. A part d'aquesta configuració feta a nivell del portal, la relació implica que el generador , quan opera amb KeyOne LRA, verifica les signatures realitzades en l'operació d'aprovació per part de l'operador.

Aquesta validació queda reflectida en el KeyOne LRA alhora de mostrar les peticions pendents de generar amb un codi de colors tal com :

- Petició verificada en color verd
- Petició no verificada en color vermell

Per tal de poder fer aquesta validació cal construir per cada generador el conjunt de confiança dels aprovadors relacionats per poder fer la verificació de la signatura. Tècnicament es tracta de construir un PSS per cada generador amb tots els certificats dels aprovadors relacionats.

Aquesta operació és realitza periòdicament (cada 30 minuts) i en un procés en segon pla, deixant els elements PSS en la base de dades on la KeyOne LRA els recupera.

4.6 Generació de documentació

A continuació es descriuen els diferents aspectes que permeten la gestió i generació de la documentació necessària durant els processos de generació dels certificats digitals.

4.6.1 Requeriments

Dins la gestió de documents es compleixen els següents requeriments.

- La documentació és genera a partir d'una sèrie de **documents base** en format RTF
- El procediment de personalització és realitza a partir de la substitució de cadenes concretes de text que estan dins el document RTF. Aquestes cadenes comencen sempre amb els caràcters **$$**
- El sistema permet definir quins documents es generen per cada tipus de certificat. Els tipus de documents definits son:
    - **FL** – Full de lliurament
    - **CL** – Carta de lot
    - **CP** – Carta de PIN. Només aplica a les LRAs amb generació de PINs amb impressora d'agulles.
    - **AL** – Albarà de lliurament

- **PIN_PUK_TEMPLATE** – Document de PIN i PUK. Només aplica a les LRAs amb generació de PINs amb impressora LASER.

- El sistema permet definir quins grups de document, en funció de la política, s'envien a cada LRA en funció del seu codi de ER.
- El procés de substitució es realitza en dos punts
  - En el procés de generació dels documents que s'envien a una LRA. En aquest punt es realitzen les substitucions de les dades fixes que depenen de la ER. Per conveni, aquestes dades es poden identificar dins el document RTF per una cadena que del tipus **$$MAJUSCULES.**
  - En el procés de generació dels certificats. En aquest punt, i a partir dels documents que es reben de la CA, es realitzen les substitucions de les dades que depenen de la petició de certificació que estem generant. Per conveni, aquestes dades es poden identificar dins el document RTF per una cadena que del tipus **$$minuscules.**

4.6.2 Elements tècnics del mòdul

La ubicació del fitxers RTF serà dins del directori:
\ScriptsLRA\EC_XX\dscripts_V3\docsBase

Existiran tants fitxers com plantilles de documents diferent. En una primera versió tenim la següent llista.

- CATCERT_CDS-CDA-CDSDC-CDP_CL.rtf
- CATCERT_CDS-CDP-CDA-CDSDC_FL.rtf
- CATCERT_CPISR-CPISRC-CESR_AL.rtf
- CATCERT_CPISR-CPISRC-CESR_CL.rtf
- CATCERT_CPISR-CPISRC-CESR_CP.rtf
- CATCERT_CPISR-CPISRC-CESR_FL.rtf
- CATCERT_PIN_PUK_TEMPLATE.rtf
- GENERIC_CDS-CDA-CDP-CDSDC_CL.rtf
- GENERIC_CDS-CDP-CDA-CDSDC_FL.rtf
- GENERIC_CPISR-CPISRC-CESR_AL.rtf
- GENERIC_CPISR-CPISRC-CESR_CL.rtf
- GENERIC_CPISR-CPISRC-CESR_CP.rtf
- GENERIC_CPISR-CPISRC-CESR_FL.rtf
- GENERIC_PIN_PUK_TEMPLATE.rtf

On els fitxers que comencem amb CATCERT_* pertanyen a les plantilles utilitzades per la ER de la AOC (codi 000) i els fitxers que comencen per GENERIC_* pertanyen a les plantilles utilitzades per la resta de ER.

Aquests documents poden ser diferents per cada EC.

Per altra banda dins el directori ScriptsLRA\EC_XX\dscripts_V3\configAmbits existirà un fitxer per cada ER(xxx.txt). EL contingut d'aquest fitxers ha de ser.

AMBIT_DESC = Descripció de la LRA
AMBIT_ADRESS = Adreça postal
AMBIT_POB = Població
AMBIT_CP = Codi Postal
AMBIT_RESP = Nom i cognoms del responsable
AMBIT_TEL = Telefon de contacte
AMBIT_CIF = CIF de la LRA

AMBIT_GRUP = Nom del grup de documents (Per exemple GENERIC, ORGT o CATCERT)

Dins el mateix directori també existirà un fitxer de definició (GRUP_NOM_GRUP.config) per cada etiqueta diferent que hi pugui haver dins els camp AMBIT_GRUP dels anteriors fitxers.

Aquest fitxer contenen els següents paràmetres.
LLISTA_POLITIQUES = Llistat de les polítiques que poden generar les LRAs d'aquest grup. També cal afegir l'element PIN_PUK si la LRA pot generar targetes.

Per exemple:
LLISTA_POLITIQUES = CDA_1,CDS_1,CDP_1,CDSDC_1,CESR_1,CPISR_1_O,CPISRC_1_O,PIN_PUK

Per cada element de la llista anterior tenim dos paràmetres.

itemLlista_DOCS = Llista de identificadors de documents que pot generar aquesta política.
itemLlista _DESC = Descripció de la política que es farà servir en els documents.

Per exemple:
CPISR_1_DOCS = FL_CARD,CL_CARD,AL_CARD,CP_CARD
CPISR_1_DESC = CPISR+CPX

Finalment el fitxer conté la definició de cadascun del identificadors dels fitxers de les variables xxx_DOCS. Aquesta definició conté els següents camps.

DOC_BASE = nom de la plantilla RTF
DOC_SUBST = Conjunt de substitucions a realitzar abans de generar el codi per la ER relacionada.

Per exemple:
```
FL_CARD_DEFINICIO <<<!  EOF_definicioDoc -$
        DOC_BASE = GENERIC_CPISR-CPISRC-CESR_FL.rtf
        DOC_SUBST <<<! EOF_docSubst -$
                doc = ${subst:$$NOM_ER:${escapecolon:${AMBIT_DESC}}:${doc}}
                doc = ${subst:$$ADRESS_ER:${escapecolon:${AMBIT_ADRESS}}:${doc}}
                doc = ${subst:$$CP_ER:${escapecolon:${AMBIT_CP}}:${doc}}
                doc = ${subst:$$POB_ER:${escapecolon:${AMBIT_POB}}:${doc}}
                doc = ${subst:$$TIPUS_CERT:${escapecolon:${${politicaItem}_DESC}}:${doc}}
        EOF_docSubst
EOF_definicioDoc
```

Una vegada situats tots els elements, l'execució de packdscripts.ws realitza els següents passos a partir del codi de la ER (xxx.txt).

a. Carregar el fitxer xxx.txt
b. Obtenir el paràmetre AMBIT_GRUP i carregar el fitxer relacionat GRUP_xxxxxx.config
c. Per cada element de la llista **LLISTA_POLITIQUES** obtenir la llista de documents associats (**itemLlista_DOCS**) i generar-los a partir del documents base (**DOC_BASE**) realitzant les substitucions definides (**DOCS_SUBST**).
d. Finalment el posa dins el conjunt d'scripts de la LRA amb el nom de la política i tipus de document adient.

Al finalitzar aquesta fase els documents estan personalitzats amb les dades que no depenen de la generació del certificat corresponent. Per fer la resta de la personalització del document cal definir-ho dins el fitxer de política (idPoliocy.ws), situats tan a la màquina del portal del SCD.

Caldrà, en cada cas, realitzar les assignacions corresponents a totes les variables $$minuscula dels documents.

Aquestes assignacions es realitzen dins les definicions com per exemple.

```
${policyId}_FL <<<! EOF -$
        doc = ${subst:$$resp_nom:${escapecolon:${resp_nom}}:${doc}}
        doc = ${subst:$$resp_nif:${resp_nif}:${doc}}
        doc = ${subst:$$nom:${escapecolon:${cn} ${cn2}}:${doc}}
        doc = ${subst:$$tipus_doc:${doc_type}:${doc}}
        doc = ${subst:$$doc_num:${doc_num}:${doc}}
        doc = ${subst:$$email:${ea}:${doc}}
        doc = ${subst:$$org:${escapecolon:${o}}:${doc}}
        doc = ${subst:$$ou:${escapecolon:${ou}}:${doc}}
        doc = ${subst:$$cif_org:${cif_org}:${doc}}
        doc = ${subst:$$pob:${escapecolon:${resp_pob}}:${doc}}
        doc = ${subst:$$data:${data}:${doc}}
        doc = ${subst:$$sn1:${serial1}:${doc}}
        doc = ${subst:$$sn2:${serial2}:${doc}}
        doc = ${subst:$$notafter1:${notafter1}:${doc}}
        doc = ${subst:$$notafter2:${notafter2}:${doc}}
        doc = ${subst:$$notbefore1:${notbefore1}:${doc}}
        doc = ${subst:$$notbefore2:${notbefore2}:${doc}}
        doc = ${subst:$$policy1:${policy1}:${doc}}
        doc = ${subst:$$policy2:${policy2}:${doc}}
        doc = ${subst:$$idsusp:${idsusp_clear}:${doc}}
EOF
```

Aquestes definicions poden dependre de cada tipus de certificat i quines dades tenim disponibles. El que cal verificar es que totes les variables definides a la plantilla RTF son substituïdes per algun valor.

Finalment i durant el procés de generació del certificat, KeyOne LRA , generarà el document definitiu a partir del document base que rep de la CA i substituït el valor de les variables en minúscula seguint les regles definides dins el fitxer de política.

4.7 Notificacions del sistema

A continuació es descriuen totes les comunicacions que el sistema del SCD cal que enviï. Per cadascuna d'elles és descriu en les mateixes característiques:

- Emissor [from]
- Destinataris [To]
- Acció que la desencadena
- Descripció del contingut
- Cal signar i/o xifrar
- Altres consideracions

4.7.1 Comunicació de Nova Petició

Emissor: scd@aoc.cat
Destinataris: Tots els aprovadors relacionats de l'ER a la que pertany el peticionari + Responsable de l'ER
Acció: Introducció de peticions per part dels peticionaris
Contingut: Identificadors/dades de les peticions introduïdes
Signat: No
Altres consideracions:
Les peticions introduïdes al sistema de manera massiva no generen aquesta notificació.

4.7.2 Comunicació d'Aprovació

Emissor: scd@aoc.cat
Destinataris: Tots els generadors relacionats de l'ER a la que pertany el aprovador + Responsable de la ER
Acció: Aprovació de peticions per part dels aprovadors
Contingut: Identificadors/dades de les peticions introduïdes
Signat: No
Altres consideracions:
No cal enviar cap comunicació si l'aprovació és fa des de la LRA

4.7.3 Comunicació de Denegació

Emissor: scd@aoc.cat
Destinataris: Peticionari que ha introduït la petició
Acció: Denegació de peticions per part dels aprovadors
Contingut: Identificadors/dades de les peticions denegada
Signat: No
Altres consideracions:
Si la petició és introduïda de manera automàtica caldrà assegurar que l'adreça que conté el CDA utilitzat és real i accessible per els operadors.

4.7.4 Comunicació de Canvi d'estat

Emissor: scd@aoc.cat
Destinataris: Posseïdor de claus
Acció: Revocacions/suspensions/habilitacions de certificats per part dels gestors de certificats
Contingut: Identificadors/dades del certificat afectat
Signat: Sí
Altres consideracions:
Per evitar l'enviament de correus electrònics en cas d'errors en la generació, etc. només s'aplicarà als certificats amb estat lliurat. Cal tenir en compte que tampoc afecta els certificats esclaus.

4.7.5 Comunicació de PIN&PUK

Emissor: scd@aoc.cat
Destinataris: Posseïdor de claus
Acció: S'ha marcat com a lliurat el certificat per part del Administrador de la ERV
Contingut: Identificadors/dades del certificat afectat, PIN i PUK en cas de targetes o contrasenya del PKCS #12 en altres casos.
Signat: Sí
Altres consideracions:
Només si estan lliurats
No afecta els certificats esclaus

4.7.6 Recordatori d'Aprovació

Emissor: scd@aoc.cat
Destinataris: Aprovadors relacionats a les peticions que estan pendents d'aprovar
Acció: Procés que miri si les peticions pendents d'aprovar superen el límit de temps configurat. Aquest temps tindrà un ordre de magnitud de dies.
Contingut: Identificadors/dades de les peticions.
Signat: No
Altres consideracions:
Es consideren 3 recordatoris, als 3, 5 i 15 dies.

4.7.7 Recordatori d'eliminació

Emissor: scd@aoc.cat
Destinataris: Aprovadors relacionats a les peticions que estan pendents d'aprovar.
Peticionari de la petició
Acció: Procés que miri si les peticions superen el límit de 90 dies des de la darrera acció dins el sistema.
Contingut: Identificadors/dades de les peticions.
Signat: No
Altres consideracions:
Ha d'existir la possibilitat de deshabilitar aquesta opció ja que hi ha Ecs que tenen moltes peticions en cartera i que són correctes. Actualment aquest cas el trobem a EC-URV i EC-UR per els certificats de la UPC.

4.7.8 Recordatori de Generació

Emissor: scd@aoc.cat
Destinataris: Generadors relacionats a les peticions que estan pendents de generar
Acció: Procés que miri si les peticions pendents de generar superen el límit de temps configurat. Aquest temps tindrà un ordre de magnitud de dies.
Contingut: Identificadors/dades de les peticions.
Signat: No
Altres consideracions:

4.7.9 Recordatori de Lliurament

Emissor: scd@aoc.cat
Destinataris: Administrador de l'ERV relacionats als certificats pendents de lliurar
Acció: Procés que miri els certificats pendents de lliurar i que superen el límit superen el límit de temps configurat. Aquest temps tindrà un ordre de magnitud de dies.
Contingut: Identificadors/dades de les peticions.
Signat: No
Altres consideracions:
Es consideren 3 recordatoris, als 3, 5 i 15 dies després de la generació.

4.7.10 Recordatori de Renovació – 60 dies

Emissor: scd@aoc.cat
Destinataris: Posseïdor de claus i/o responsable de servei de la ERV

Acció: Procés que miri si els certificats generats en estat vàlid i que caduquen durant els propers **60** dies
Contingut: Identificadors/dades dels certificats
Signat: Sí
Altres consideracions:
- El cos del missatge és diferent per l'Administrador de servei de la ERV i posseïdor

4.7.11 Recordatori de Renovació – 30 dies

Emissor: scd@aoc.cat
Destinataris: Posseïdor de claus i/o responsable de servei de la ERV
Acció: Procés que miri si els certificats generats en estat vàlid i que caduquen durant els propers **30** dies. No s'enviarà si entre el de 60 dies i aquest s'ha renovat o revocat el certificat.
Contingut: Identificadors/dades dels certificats
Signat: Sí
Altres consideracions:
- El cos del missatge és diferent per l'Administrador de servei de la ERV i posseïdor

4.8 Generació d'informes ONLINE

Des del portal del SCD, els operadors amb rol adient podran obtenir, en format .csv, determinats informes sobre els certificats dels seus ens associats. Aquest informes, una vegada demanats per part de l'operador, es generen en segon pla. Una vegada generats el sistema notifica al operador que pot accedir al mateix portal del SCD per procedir a la seva descàrrega.
Les característiques d'aquests informes son les següents:

1. Informes disponibles
    a. Extracció global de certificats
    b. Informe de certificats vàlids
    c. Informe de certificats revocats
    d. Informe de certificats suspesos
    e. Informe de certificats que caduquen en els propers 2 mesos
2. Les dades dels informes obtinguts son per EC i contenen les dades dels ens que té associat l'operador, només els operadors de la ER amb codi 000 obtenen informes que contenen la totalitat de certificats de la EC
3. El període de generació en segon pla és un màxim de 24 h
4. Els informes es lliuren en format .csv comprimits en zip
5. Cada informe es pot demanar un màxim d'una vegada al dia
6. Els operadors disposen de l'històric d'informes demanats i generats

4.9 Generació d'informes BACKOFFICE

El sistema genera informes en format CSV , periòdicament i de manera automàtica. Els informes que generats son el següents:

Extracció DWH

Periodicitat: Setmanal
Destí: DWH AOC
Dades: extracció global, totes les EC
Formats: .csv i .rar

Extracció Justícia

Periodicitat: Diària
Destí: Departament de Justícia, descàrrega i pujada per FTP
Dades: Extracció de tots els certificats de EC-SAFP amb codis d'ens 9611290004, 7515090709 i 9611290315
Formats: .csv i .rar

Extracció UPC

Periodicitat: Diària
Destí: UPC, descàrrega WEB (autenticació amb certificat)
Dades: Certificats de EC-UR amb Organització igual a 'Universitat Politecnica de Catalunya','Universitat Politècnica de Catalunya','UPC','UPCnet'. EC-UR
Formats: .csv i .rar

Extracció UB

Periodicitat: Diària
Destí: UB, descàrrega WEB (autenticació amb certificat)
Dades: Certificats de EC-UR amb codi d'ens igual a CINV00247. EC-UR
Formats: .csv i .rar

Extracció URV

Periodicitat: Diària
Destí: URV, descàrrega WEB (autenticació amb certificat)
Dades: Tots els certificats de EC-URV i tots els certificats de EC-UR amb codi d'ens igual a CINV00215.
Formats: .csv i .rar

4.10 Recuperació de PIN/PUK

Aquesta part del portal SCD permet recuperar els codis PIN i PUK **originals** de les targetes emeses en posterioritat de la primera meitat de l'any 2009.

Es tracta d'una part del portal SCD que no requereix autenticació amb certificat digital i que permet als posseïdors de les claus rebre en el correu electrònic contingut dins el certificat i **només en aquesta adreça** els **codis originals** que es varen fixar en el moment de la generació dels certificats.
També es permesa la recuperació de les paraules de pas del fitxers PKCS#12, per certificats emesos en aquest suport.

Les dades necessàries per poder activar aquest reenviament són:

- DNI/NIF
- Correu electrònic
- Codi de suspensió, disponible en el document d'acceptació dels certificats
- Codi CAPTCHA

4.11 Certificats T-CATP

El sistema permet la generació de certificats personals en suport software (PKCS#12). Aquest certificats per la seva naturalesa comporten una sèrie de modificacions i adaptacions als fluxos estàndards definits a la plataforma.

A continuació es detallen les característiques del tipus de certificat T-CAT P:

1. És un certificat personal, amb usos d'autenticació, signatura i xifrat
2. La mida de les claus és de 2048 bits o superior
3. El parell de claus és generat per l'Entitat de certificació
4. L'Entitat de certificació elimina la clau privada, una vegada hagi estat lliurada a l'usuari
5. El format de lliurament és un fitxer PKCS #12
6. La EC xifra les claus privades generades amb una clau d'ofuscació custodiada per un HSM, per evitar que siguin recuperables directament de la base de dades
7. El destí de les claus, especificat en el moment de l'aplicació, pot tenir tres valors:
    a. **Usuari**. El propi usuari es descarregarà el certificat i rebrà la paraula de pas per la instal·lació del PKCS#12
    b. **Aplicació**. Un sistema automatitzat es descarregarà els PKCS#12 i els habilitarà per el seu ús en una plataforma de signatura centralitzada externa de la AOC. L'usuari rebrà la paraula de pas del PKCS#12 que li permetrà l'activació de la clau en la plataforma esmentada.
    c. **Servei Targeta Virtual**. En aquest cas, la PKI interaccionarà amb el Servei de Targeta Virtual de TrustedX i aprovisionarà automàticament el certificat dins aquesta plataforma. L'usuari caldrà que defineixi la paraula de pas per l'ús del servei.

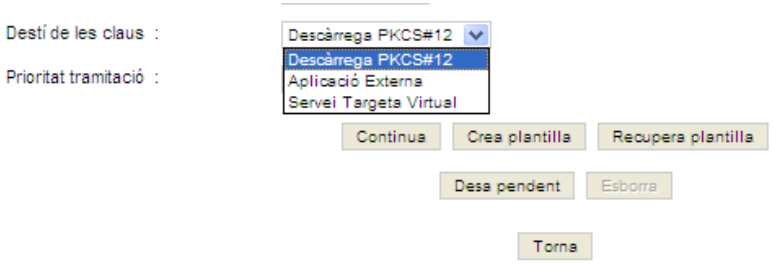
A continuació es descriuen els canvis en els fluxos estàndard.

4.11.1 Petició

El processos de petició d'un certificat tipus T-CAT P són els mateixos que es segueixen actualment amb els certificats T-CAT. Per tant l'origen de la petició pot ser:

- Des de EACAT
- Des dels propis formularis del servei SCD

En el procés de petició caldrà informar, a part de les dades del posseïdor de les claus, el destí de les claus.



4.11.2 Aprovació

El procés d'aprovació d'un certificat tipus T-CAT P és el mateix que es segueix actualment amb els certificats T-CAT, per tant es realitzarà des dels propis formularis del servei.

4.11.3 Generació

Una vegada aprovats els certificats, aquests es generen de la següent manera.
Un procés programat, resident dins la pròpia EC, accedeix a la base de dades i selecciona els certificats tipus T-CAT P en estat aprovat i, per tant, pendents de generar. En aquest moment el sistema fa les següents accions:

- La EC genera un parell de claus i el corresponent certificat.
- Genera un PKCS #12 amb una contrasenya aleatòria que també guarda.
- El PKCS #12 i la seva contrasenya es guarden dins una taula de la base de dades [TCATP_DATA] xifrada amb una clau del HSM. Aquesta taula no és pròpia del producte KeyOne CA.
- Es genera el full de lliurament i es publica al servei SCD
- S'envia un correu-e al posseïdor del certificat indicant que s'ha generat un certificat al seu nom. **NO** s'annexa el full de lliurament.
- Es deixa disponible als responsables del servei de l'ens al que pertany el posseïdor el certificat per procedir al seu lliurament

Aquest procés s'executa cada 2 minuts. Aquest interval de temps es pot configurar mitjançant un dels paràmetres del sistema.

4.11.4 Lliurament

El lliurament es basa en diferents passos:

A. El posseïdor es persona davant del responsable de servei.
B. El responsable accedeix a la carpeta del subscriptor i descarrega el full de lliurament.
C. El posseïdor signa el full de lliurament.
D. En el cas que el destí de les claus sigui l'usuari o el servei de targeta virtual, el posseïdor introdueix un Codi personal que només coneix ell i que necessitarà en el moment de la descàrrega o activació de la targeta virtual. Aquest codi haurà de tenir com a màxim 8 caràcters (mínim 1 caràcter) entre números i/o lletres. En l'altre cas, on el destí és l'aplicació externa aquest codi no és necessari.
E. El responsable marca el lliurament del certificat a l'aplicació.
F. En aquest moment el sistema guarda a la base de dades juntament amb el PKCS #12 ofuscat, el PIN del PKCS #12 generat pel sistema també ofuscat amb la mateixa clau que custodia un HSM i, per últim, el HASH del Codi de descàrrega personal que coneix només l'usuari. En aquest mateix punt, s'habilita la descàrrega del PKCS #12 o l'activació del servei de targeta virtual.

4.11.5 Descàrrega

Aquest procediment, executat per part de l'usuari, només aplica si el destí de les claus és PKCS #12. El procediment és el següent:

A. El posseïdor, ja en el seu lloc de treball, accedeix a la pàgina de descàrrega/activació de T-CAT P (URL amb SSL però sense autenticació).
B. Introdueix el seu correu-e contingut en el certificat, el NIF/NIE contingut en el certificat, el Codi de suspensió (es troba dins el full de lliurament) i el Codi de descàrrega personal. El sistema li retorna el fitxer PKCS #12.
C. Posteriorment, l'usuari rebrà per correu-e el PIN del fitxer PKCS #12.
D. El sistema controla el número de descàrregues i el període de temps en què es poden realitzar. Es configura amb una possible descàrrega durant els 10 dies posteriors a l'activació de la pròpia. Com a excepció, i per tal d'evitar possibles incidències, els 5 minuts següents al moment en que l'usuari efectua la primera

descàrrega estan exempts de la limitació de número de descàrregues. És a dir, es podrà prémer el botó de descàrrega tants cops com es necessiti sense que cap error aparegui. Les situacions que es volen evitar són per exemple que l'usuari faci "Obrir" en comptes de "Desar" en el diàleg i torni a començar per poder guardar el PKCS #12, o que guardi el PKCS #12 però no recordi on i vulgui tornar a guardar-lo en un lloc específic.

En aquesta etapa es defineixen dos períodes de retenció: el de lliurament i el de descàrrega.

- Per una banda, el període de retenció de lliurament del PKCS #12 és de 30 dies des de la generació. És a dir, si no es lliura en aquest període el PKCS #12 i la paraula de pas s'esborra de la base de dades.
- Per una altra banda, el període de retenció de descàrrega del PKCS #12 és de 10 dies, màxim de temps que pot transcórrer entre que el responsable del servei marca com a entregat el full de lliurament i que l'usuari posseïdor descarrega el PKCS #12. Tanmateix, si aquesta condició no s'acompleix el PKCS #12 i la paraula de pas s'esborra de la base de dades.

En tots dos casos, el certificat és revocat abans d'esborrar el PKCS #12 de la base de dades.
Per tal d'evitar que el PKCS #12 s'esborri de la base de dades per l'acompliment d'aquests dos períodes i haver de tornar generar una nova petició, s'envien correus-e recordatoris tant al responsable de servei durant l'etapa de lliurament com a l'usuari en període de descàrrega. En concret s'envien dos recordatoris de lliurament (el dia 7 i el dia 21 des de la generació) i dos recordatoris de descàrrega (el dia 3 i el dia 7 des del lliurament).

En cas d'oblidar o perdre el correu-e amb el PIN del PKCS #12, l'usuari tindrà la opció de recuperació d'aquest a través d'un formulari web.

4.12 Administració del sistema

A continuació és descriuen les opcions d'administració del sistema, que es poden realitzar des del portal del servei SCD.

Els operadors amb aquest rol estan configurats en una ACL a partir del seu número de sèrie del seu certificat. Un operador amb aquest rol pot administrar qualsevol de les ECs del sistema, excepte EC-IDCAT que té la seva pròpia gestió en la capa RA.

A part de conèixer la operativa d'aquesta part també pot ajudar a tenir un aproximació a les tasques d'administració que calen per gestionar el correcte funcionament de la infraestructura.

4.12.1 Gestió de ER

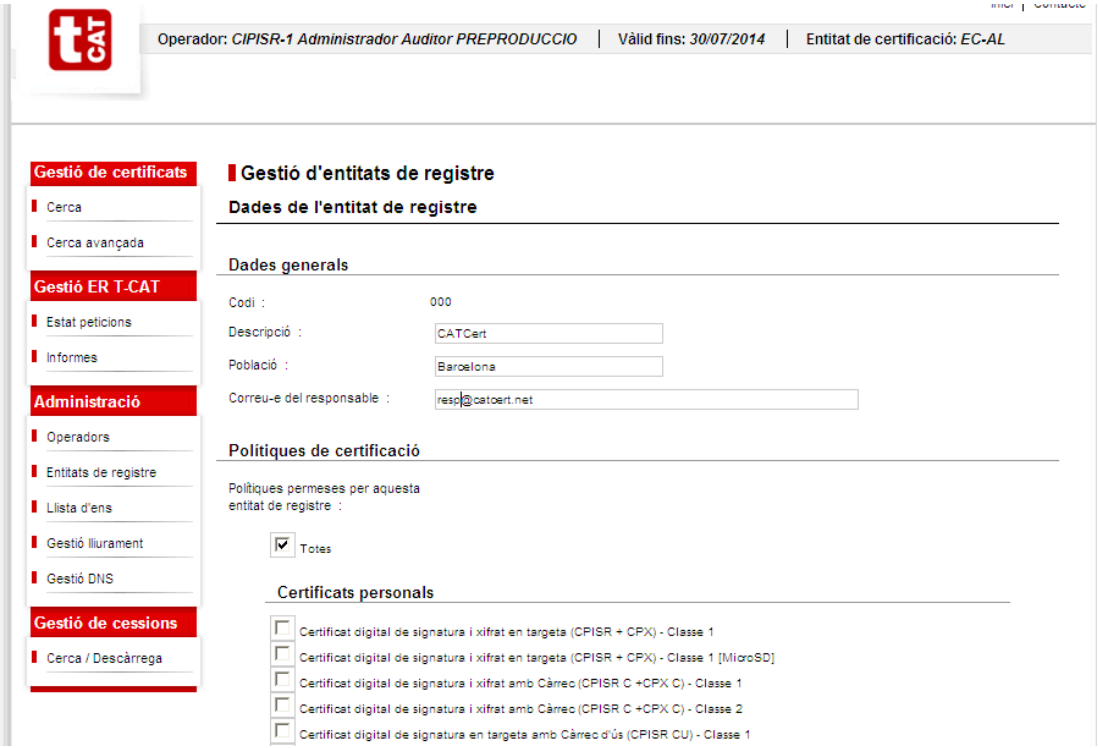
Permet la gestió de les dades relacionades amb cada ER. La relació de ER actualment és la següent:

Entitat de certificació	Número de ERs
EC-AL	60
EC-SAFP	6
EC-PARLAMENT	1

EC-URV	8
EC-URV	1
EC-IDCAT	n/a

L'operador pot realitzar les següents operacions sobre les ER de cada EC.

- Cerca
- Alta (una nova ER requereix també d'altres procediments tècnics, jurídics i logístics)
- Baixa
- Modificació
- Fixar els següents paràmetres per cada entitat de registre
  - Codi
  - Descripció
  - Llista de correus-e de responsables relacionats a aquesta ER
  - Llista de polítiques disponibles per aquesta ER
  - Llista de dissenys de targeta disponibles per aquesta ER
  - Llista de ens a aplicar en el filtre dels operadors de la ER



4.12.2 Gestió de operadors

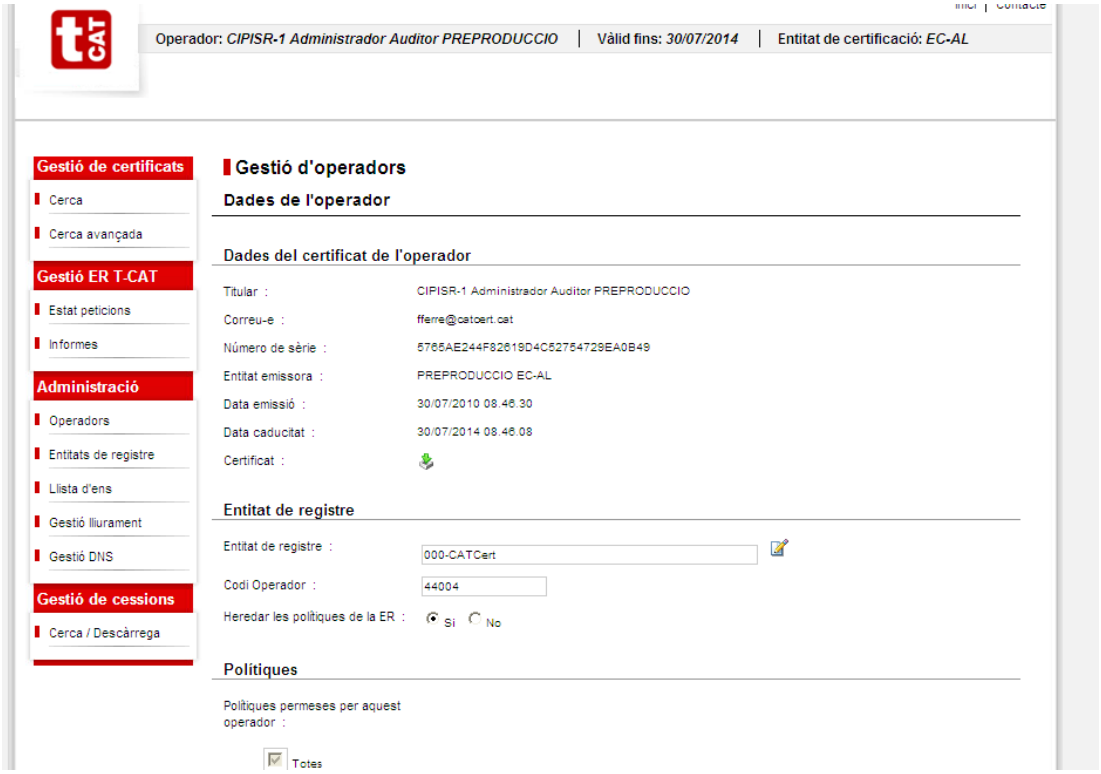
Permet la gestió dels operadors, els seu rol, les seves dades, la relació amb les ERs , etc.
La número d'operadors actuals per EC és el següent:

Entitat de certificació	Número d'operadors del sistema
EC-AL	458
EC-SAFP	119
EC-PARLAMENT	121
EC-UR	341
EC-URV	157

EC-IDCAT	n/a

L'operador pot realitzar les següents operacions durant la gestió d'operadors.

- Cerca
- Alta. Per donar d'alta operador farà falta tenir disponible el fitxer .crt que conté el certificat d'autenticació (normalment CIPISR) del mateix
- Baixa
- Modificació
- Fixar els següents paràmetres per cada entitat de registre
    - Codi operador
    - Correu electrònic. S'obté el Correu-e de l'operador a partir de les dades del certificat
    - ER a la que pertany, només pot ser una.
    - Rol de l'operador
        - Introduir peticions
        - Aprovar peticions
        - Gestionar certificats (Suspendre/habilitar o Revocar/Suspendre/habilitar)
        - Generar certificats. Aquest rols també precisen, per seguretat, de configuració addicional directament a KeyOne CA.
        - Administrador ERV T-CAT
        - Dipositari AOC
    - Permisos especials
        - Importar peticions
        - Revocació automàtica
        - Accés al sistema de Lots
    - Llista de polítiques disponibles per aquest operador. Es poden heretar de la configuració de la ER
    - Llista de correu-e d'operadors. Aplica a notificacions entre operadors peticionaris, aprovadors i generadors.
    - Operadors Relacionats. Aplica a rol Aprovador i generador i fixa la llista d'aprovadors acceptats per cada generador.



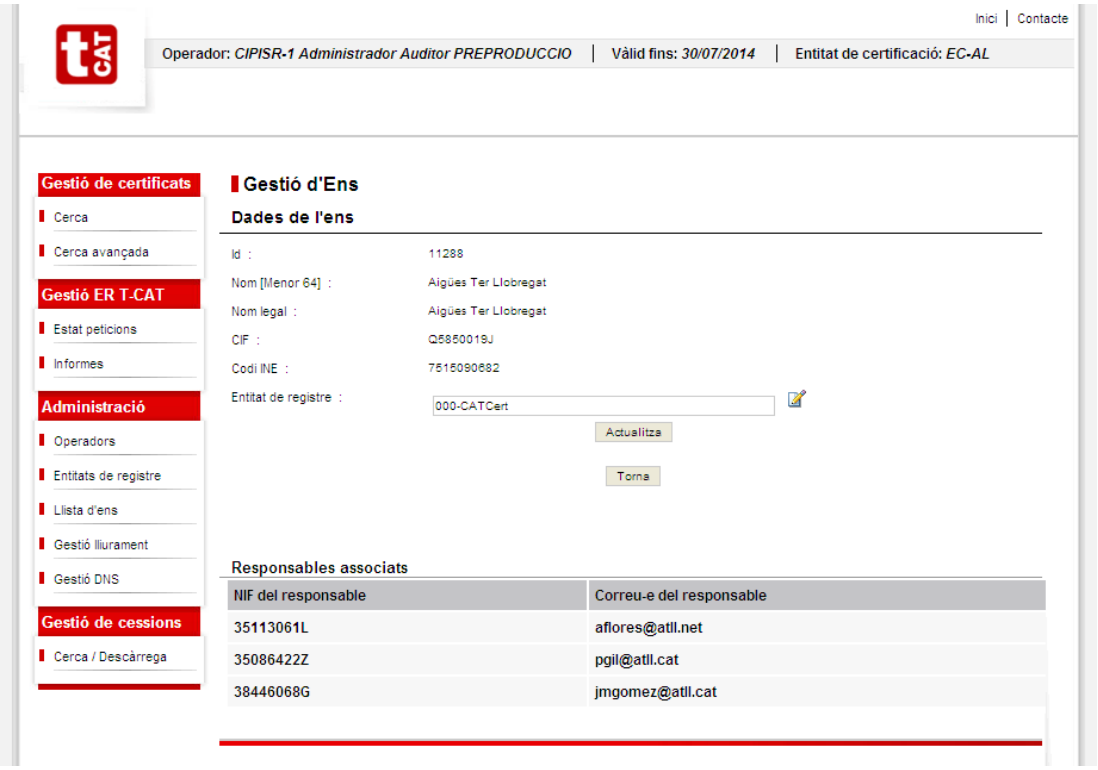
4.12.3 Llista d'ens

Permet la gestió dels ens per cada EC. En aquest cas la font és externa i només es permet l'assignació de cada ens a una ER determinada. Si la seva ER és la que té codi 000, no cal fer res. El número d'ens actuals per EC és el següent:

Entitat de certificació	Número d'ens
EC-AL	1817
EC-SAFP	875
EC-PARLAMENT	4
EC-UR	68
EC-URV	2
EC-IDCAT	n/a

L'operador pot realitzar les següents operacions durant la gestió d'ens.

- Cerca
- Visualització de responsables assignats
- Fixar els següents paràmetres per cada entitat de registre
    - ER assignada

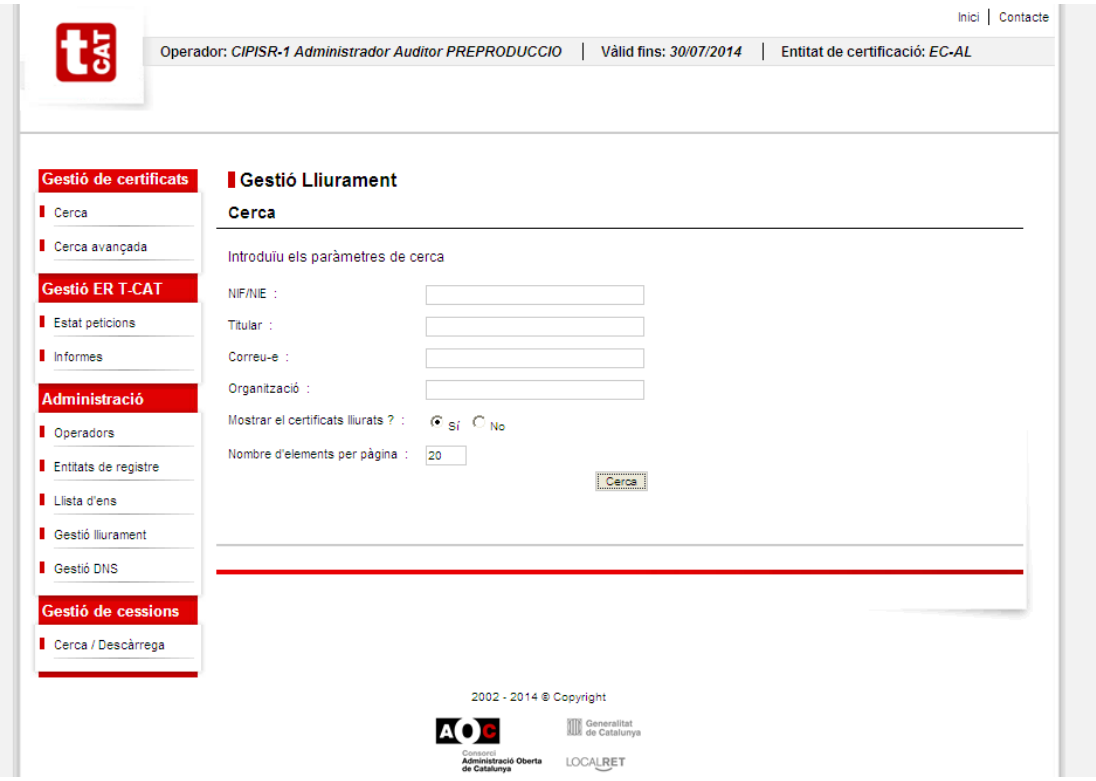


4.12.4 Gestió Lliurament

Permet la visualització de l'estat de lliurament de qualsevol certificats del sistema. És tracta d'una opció utilitzada sobretot per la gestió d'incidències degudes al procés de lliurament que han de fer el responsables de servei de cada ens.

L'operador pot realitzar les següents operacions:

- Cerca
- Visualització del certificats
- Visualitzar la documentació
- Activar l'enviament del PIN/PUK o paraula de pas del PKCS#12 segons correspongui



4.13 Mòdul de cessió

Aquest mòdul incorpora la possibilitat de delegar a un tercer la descàrrega de les claus, per els tipus de certificat de Segell electrònic, CEIXA i CDA . Això fa mes eficient i segur la gestió d'aquests tipus de certificats quan aquests són utilitzats per serveis i aplicacions de la pròpia AOC.

En aquest cas, cal indicar en la petició del certificat, que aquest està cedit a la AOC. Aquest certificats modificaran part del seu flux estàndard amb els següents canvis:

- Quan es genera el certificat, el subscriptor podrà veure el certificat en la llista però no pot descarregar la clau privada
- El Consorci AOC té una opció dins la carpeta del subscriptor per descarregar totes les claus privades cedides, així com sol•licitar el corresponent PIN (una opció a la que només tindrà accés qui Operacions determini – operador amb rol 'Dipositari AOC').
- En les opcions disponibles per el responsable de serveis es deshabilita la possibilitat de descàrrega del P12 per els certificats d'aquest tipus. El responsable continua fent l'acte de 'lliurament' però aquest no implica ni que pugui descarregar el P12 ni tampoc que el sistema enviï el PIN. Per fer aquest acte ha d'haver signat el nou "full de lliurament" de cessió/dipòsit.
- La gestió del cicle de vida del certificat (emissió, revocació, suspensió, etc..) segueix essent responsabilitat plena de l'ens titular.
- El sistema garanteix que no s'ha baixat mai el p12 des de l'ens que el sol·licita, evitant còpies.

L'operador amb rol Dipositari AOC pot realitzar les següents operacions:

- Cerca
- Lliurament i Descàrrega de certificats. Com a conseqüència rebrà el correu electrònic amb la paraula de pas per la seva utilització/instal·lació.

5 Altres mòduls

A continuació es descriuen altres mòduls (més tecnològics) que aporten a la infraestructura el compliment de més requeriments.

5.1 Control d'unicitat

El control d'unicitat evita la generació de dos certificats vàlids del mateix tipus al mateix titular.

Aquest mòdul compleix els següents requeriments.

- La regla d'unicitat, conjunt de dades que configuren el valor que no pot repetir-se, és configura per cada perfil en el fitxer idPolicy.ws
- El sistema controla la unicitat en dos fases, la de peticionari i finalment a la de generació.
- El sistema permet configurar el període de temps anomenat de renovació que permet saltar-se la regla d'unicitat. Actualment fixat a dos mesos.
- El control en la fase de petició es realitza tan en el sistema ONLINE com en el sistema de LOTS. En aquesta fase també es controla que no hi hagi unicitat entre peticions de certificació pendents de generar, amb el mateix criteri.
- En cas de trobar-se un certificat que compleixi la unicitat s'informa a l'operador que no és pot realitzar l'operació i es retorna el número de sèrie del certificat que la provoca.
- Addicionalment, en la fase de petició, també s'indica al operador, en aquest cas en mode informatiu, si hi ha certificats o peticions dins el sistema amb al mateix codi de document, normalment DNI.

5.2 Generació i publicació de CRLs

El sistema genera CRLs de durada 7 dies amb els certificats revocats i suspesos.
Cada EC genera un mínim de una CRL cada 24 hores.

Una vegada generades es publiquen de manera automàtica, a través d'una connexió segura SSH, a tres servidors externs.

Maquinari físic

CA Root: HP Model 290 G1 amb HSM USB Edge	SW Linux, EJBCA, MySQL
CA Root CONT: HP Model 290 G1 amb HSM USB Edge	SW Linux, EJBCA, MySQL

Dispositius criptogràfics (HSM)

HSM-PKI-PRO-1	HSM Connect XC, NCIPHER	NH2089	EC2A-03E0-D947	46-SC0577	HSM de PKI	
HSM-PKI-PRO-2	HSM Connect XC, NCIPHER	NH2089	ED16-05E0-D947	46-SC4384	HSM de PKI	
CA Root: HP Model 290 G1 amb HSM USB Edge	HSM USB Edge	HSM			Linux	EJBCA, MYSQL
CA Root CONT: HP Model 290 G1 amb HSM USB Edge	HSM USB Edge	HSM			Linux	EJBCA, MYSQL

Codi Font en PHP de IDCAT (GIT)
Dump de BD Mysql IDCAT
Codi Font en PHP de OSIRIS (GIT)
Dump de BD Mysql OSIRIS
Impressores
Stock targetes
Stock de material d'oficina: sobres, cartes, cintes d'impressora
Procediment intern de gestió de sol·licituds
Targetes d'Operacions (revocació)
Indicadors de volumetries dels serveis
PCs per les ER

Ens	C.P.	Població	CIF	Id. Equip	Codi Àmbit	Descripció	Marca	Model
Ajuntament de Castelldefels	8860	Castelldefels	P0805500F	ER-001	101	CPU Estació RRA	HP	DC5100/P5 650 SFF
						Monitor Estació RRA	HP	L1702
						Lector de Targetes	C3PO	LTC-31
						Impressora de targetes	DATACARD	SP55
						Impressora làser per PINs i PUKs	HP	Laserjet 1320n
						Windows 7 64 bits		
Ajuntament de Girona	17004	Girona	P1708500B	ER-002	102	CPU Estació RRA	HP	DC5100/P5 650 SFF
						Monitor Estació RRA	HP	L1702
						Lector de Targetes	C3PO	LTC-31
						Impressora de targetes	DATACARD	CP60Plus
						Impressora làser per PINs i PUKs	HP	Laserjet 1320n
						Windows XP		
Ajuntament de Lleida	25007	Lleida	P2515100B	ER-003	103	CPU Estació RRA	HP	DC5100/P5 650 SFF
						Monitor Estació RRA	HP	L1940G
						Lector de Targetes	C3PO	LTC-31
						Impressora de targetes	DATACARD	SP55 PLUS
						Impressora làser per PINs i PUKs	HP	Laserjet 1320n
						Windows XP		
Ajuntament de Rubí	8191	Rubí	P0818300F	BAIXA	104	CPU Estació RRA	HP	DC5100/P5 650 SFF
						Monitor Estació RRA	HP	L1702
						Lector de Targetes	C3PO	LTC-31
						Impressora de targetes	DATACARD	SP55
						Impressora làser per PINs i PUKs	HP	Laserjet 1320n
Ajuntament de Terrassa	8221	Terrassa	P0827900B	BAIXA	105	CPU Estació RRA	HP	DC5100/P5 650 SFF
						Monitor Estació RRA	HP	L1702
						Lector de Targetes	C3PO	LTC-31
						Impressora de targetes	DATACARD	SP55
						Impressora làser per PINs i PUKs	HP	Laserjet 1320n
Ajuntament de Vilanova i la Geltrú	8800	Vilanova i la Geltrú	P0830800I	ER-006	106	CPU Estació RRA	HP	DC5100/P5 650 SFF
						Monitor Estació RRA	HP	L1702
						Lector de Targetes	C3PO	LTC-31
						Impressora de targetes	DATACARD	SP55
						Impressora làser per PINs i PUKs	HP	Laserjet 1320n
						Windows XP		
Consell Comarcal de l'Alt Penedès	8720	Vilafranca del Penedès	P5800013D	ER-007	107	CPU Estació RRA	HP	Compaq 8000 ELITE
						Monitor Estació RRA	HP	LE 1901W
						Lector de Targetes	C3PO	LTC-31
						Impressora de targetes	DATACARD	CP40 PLUS
						Impressora làser per PINs i PUKs	HP	Laserjet P2055d
						Windows 7 32 bit		
Consell Comarcal de l'Alt Urgell	25700	La Seu d'Urgell	P7500006G	ER-008	108	CPU Estació RRA	HP	HP Compaq 8000 Elite
						Monitor Estació RRA	HP	L1702
						Lector de Targetes	Bit4Id	MINILECTOR
						Impressora de targetes	DATACARD	CD800
						Windows 7 32 bit		
						Impressora làser per PINs i PUKs	HP	Laserjet 1320n
Consell Comarcal del Baix Ebre	43500	Tortosa	P9300004J	ER-009	109	CPU Estació RRA	HP	Compaq 8000 ELITE
						Monitor Estació RRA	HP	LE1901W
						Lector de Targetes	C3PO	LTC-31
						Impressora de targetes	DATACARD	CP40 PLUS
						Windows 7 32 bit		
						Impressora làser per PINs i PUKs	HP	Laserjet P2055d
Consell Comarcal de la Conca de Barberà	43400	Montblanc	P9300007C	ER-009	110	CPU Estació RRA	HP	Compaq 8000 ELITE
						Monitor Estació RRA	HP	L1702
						Lector de Targetes	C3PO	LTC-31
						Impressora de targetes	DATACARD	CD800
						Windows 7 32 bit		
						Impressora làser per PINs i PUKs	HP	Laserjet 1320n
Consell Comarcal de la Garrotxa	17800	Olot	P6700007E	ER-011	111	CPU Estació RRA	HP	Compaq 8000 ELITE
						Monitor Estació RRA	HP	LE1901W
						Lector de Targetes	C3PO	LTC-31
						Impressora de targetes	DATACARD	CP40 PLUS
						Windows 7 32 bit		
						Impressora làser per PINs i PUKs	HP	Laserjet P2055d
Consell Comarcal d'Osona	8500	Vic	P5800015I	ER-012	112	CPU Estació RRA	HP	Compaq 8000 ELITE
						Monitor Estació RRA	HP	LE 1901W
						Lector de Targetes	C3PO	LTC-31
						Impressora de targetes	DATACARD	CP40 PLUS
						Windows 7 32 bit		
						Impressora làser per PINs i PUKs	HP	Laserjet P2055d
Consell Comarcal del Pallars Sobirà	25560	Sort	P7500010I	ER-013	113	CPU Estació RRA	HP	HP 280 G1
						Monitor Estació RRA	HP	L1702
						Lector de Targetes	C3PO	LTC-31
						Impressora de targetes	DATACARD	CP60
						Windows 7 64 bits		
						Impressora làser per PINs i PUKs	HP	Laserjet 1320n
Consell Comarcal de la Ribera d'Ebre	43740	Móra d'Ebre	P9300011E	ER-014	114	CPU Estació RRA	HP	HP Compaq 8000 Elite
						Monitor Estació RRA	HP	LE1901W
						Lector de Targetes	C3PO	LTC-31
						Impressora de targetes	DATACARD	CP40 PLUS
						Windwos 7 32 bits		
						Impressora làser per PINs i PUKs	HP	Laserjet P2055d
Consell Comarcal del Ripollès	17500	Ripoll	P6700004B	ER-015	115	CPU Estació RRA	HP	Compaq 8000 ELITE
						Monitor Estació RRA	HP	LE1901W
						Lector de Targetes	C3PO	LTC-31
						Impressora de targetes	DATACARD	CD800
						Windows 7 32 bits		
						Impressora làser per PINs i PUKs	HP	Laserjet P2055d
	25007	Lleida	P7500008C			CPU Estació RRA	HP	HP 280 G1
						Monitor Estació RRA	HP	L1702

Consell Comarcal del Segrià				ER-016	116	Lector de Targetes	Bit4Id	MINILECTOR
						Impressora de targetes	DATACARD	CD800
						Windows 7 64 bits		
						Impressora làser per PINs i PUKs	HP	Laserjet 1320n
Consell Comarcal de la Selva	17430	Santa Coloma de Farners	P6700002F	ER-017	117	CPU Estació RRA	HP	Compaq 8000 ELITE
						Monitor Estació RRA	HP	LE1901W
						Lector de Targetes	C3PO	LTC-31
						Impressora de targetes	DATACARD	CP40 PLUS
						Windows 7 32 bits		
						Impressora làser per PINs i PUKs	HP	Laserjet P2055d
Consell Comarcal del Tarragonès	43003	Tarragona	P9300002D	ER-018	118	CPU Estació RRA	HP	Compaq 8000 ELITE
						Monitor Estació RRA	HP	LE1901W
						Lector de Targetes	C3PO	LTC-31
						Impressora de targetes	DATACARD	CP40 PLUS
						Windows 7 32 bits		
						Impressora làser per PINs i PUKs	HP	Laserjet P2055d
Consell Comarcal de la Terra Alta	43780	Gandesa	P9300010G	ER-019	119	CPU Estació RRA	HP	HP Compaq 8000 Elite
						Monitor Estació RRA	HP	L1702
						Lector de Targetes	Bit4Id	MINILECTOR
						Impressora de targetes	DATACARD	CD800
						Windows 7 32 bits		
						Impressora làser per PINs i PUKs	HP	Laserjet 1320n
Consell Comarcal del Pla de l'Estany	17820	Banyoles	P6700010I	ER-020	121	CPU Estació RRA	HP	HP Compaq 8000 Elite
						Monitor Estació RRA	HP	LE1901W
						Lector de Targetes	C3PO	LTC-31
						Impressora de targetes	DATACARD	CP40 PLUS
						Windows 7 32 bits		
						Impressora làser per PINs i PUKs	HP	Laserjet P2055d
CATCert (1)		Barcelona		ER-000	000	CPU Estació RRA		
						Monitor Estació RRA		
						Lector de Targetes		
						Impressora de targetes		
						Impressora làser per PINs i PUKs		
Ajuntament de Santa Coloma de Gramanet	8921	Santa Coloma de Gramenet	A60517018	BAIXA	122	CPU Estació RRA	HP	DC5100/P5 650 SFF
						Monitor Estació RRA	HP	L1702
						Lector de Targetes	C3PO	LTC-31
						Impressora de targetes	DATACARD	SP55
						Impressora làser per PINs i PUKs	HP	Laserjet 1320n
Departament de Justícia	8010	Barcelona	S0811001G	ER-025	301	CPU Estació RRA	HP	DC5100/P5 650 SFF
						Monitor Estació RRA	HP	L1702
						Lector de Targetes	C3PO	TLTC4USB
						Impressora de targetes	DATACARD	CP60 Plus
						Impressora làser per PINs i PUKs	HP	Laserjet 1320n
ORGT	8028	Barcelona	P5800016G	ER-026	120	CPU Estació RRA	HP	
						Monitor Estació RRA	HP	L1740
						Lector de Targetes		Integrat al teclat
						Impressora de targetes	DATACARD	CP 40 plus
						Window 7 64 bits		
						Impressora làser per PINs i PUKs	HP	Laserjet 14250 DTN
CATCert (material)		Barcelona		ER-027		CPU Estació RRA		
						Monitor Estació RRA		
						Lector de Targetes		
						Impressora de targetes		
						Impressora làser per PINs i PUKs		
Firmaprofesional	8173	Sant Cugat del Vallès		ER-028	000	CPU Estació RRA	HP	DC8000
						Monitor Estació RRA	HP	LE1901W
						Lector de Targetes		
						Impressora de targetes	DATACARD	CD800
						Impressora làser per PINs i PUKs		
Ajuntament de Sant Feliu de Llobregat	8980	Sant Feliu de Llobregat	P0821000G	ER-029	123	CPU Estació RRA	HP	DC7700 SFF
						Monitor Estació RRA	HP	L1740
						Lector de Targetes	C3PO	LTC-31
						Impressora de targetes	DATACARD	CP 60 plus
						Windows 7		
						Impressora làser per PINs i PUKs	HP	Laserjet 2015d
Ajuntament de Mollet del Vallès	8100	Mollet del Vallès	P0812300B	ER-031	124	CPU Estació RRA	HP	DC7700 SFF
						Monitor Estació RRA	HP	L1740
						Lector de Targetes	C3PO	LTC-31
						Impressora de targetes	DATACARD	CP40
						Windows 7 64 bits		
						Impressora làser per PINs i PUKs	HP	Laserjet 2015d
Consell Comarcal del Baix Camp	43202	Reus	P9300003B	ER-032	125	CPU Estació RRA	HP	HP 280 G1
						Monitor Estació RRA	HP	L1750
						Lector de Targetes	Bit4Id	MINILECTOR
						Impressora de targetes	DATACARD	CD800
						Windows 7 64 bits		
						Impressora làser per PINs i PUKs	HP	Laserjet 2015d
Consell Comarcal de la Segarra	25200	Cervera	P7500007E	ER-033	126	CPU Estació RRA	HP	Compaq Elite 8000
						Monitor Estació RRA	HP	LE1901W
						Lector de Targetes	C3PO	LTC-31
						Impressora de targetes	DATACARD	CP 40 plus
						Windows 7 32 bits		
						Impressora làser per PINs i PUKs	HP	Laserjet 2055d
Consell Comarcal de l'Alt Camp	43800	Valls	P9300005G	ER-034	127	CPU Estació RRA	HP	HP 280 G1
						Monitor Estació RRA	HP	L1750
						Lector de Targetes	Bit4Id	MINILECTOR
						Impressora de targetes	DATACARD	CP60
						Windows 7 64 bits		
						Impressora làser per PINs i PUKs	HP	Laserjet 2015d
Ajuntament de Manresa	8241	Manresa	P0811200E	ER-037	130	CPU Estació RRA	HP	DC7700 SFF
						Monitor Estació RRA	HP	L1740
						Lector de Targetes	C3PO	LTC-31
						Impressora de targetes	DATACARD	SP55
						Windows XP		

						Impressora làser per PINs i PUKs	HP	Laserjet 2015d
Ajuntament de Badalona	8911	Badalona	P0801500J	ER-038	131	CPU Estació RRA	HP	DC7800 SFF
						Monitor Estació RRA	HP	L1750
						Lector de Targetes	Bit4Id	ACR38
						Impressora de targetes	DATACARD	CP60
						Windows XP		
						Impressora làser per PINs i PUKs	HP	Laserjet 2015d
CATCert (desenvolupament D.Cos)				LRA-39	0	CPU Estació RRA	HP	DC7700 SFF
						Monitor Estació RRA	HP	L1740
						Lector de Targetes	C3PO	LTC-31
						Impressora de targetes	DATACARD	SP55
Consell Comarcal del Maresme	8301	Mataró	P5800008D	ER-040	132	CPU Estació RRA	HP	HP 280 G1
						Monitor Estació RRA	HP	L1740
						Lector de Targetes	Bit4Id	MINILECTOR
						Impressora de targetes	DATACARD	CD800
						Windows 7 64 bits		
						Impressora làser per PINs i PUKs	HP	Laserjet 2015d
Ajuntament de Reus	43201	Reus	P4312500D	ER-041	129	CPU Estació RRA	HP	DC7800 SFF
						Monitor Estació RRA	HP	L1750
						Lector de Targetes	C3PO	LTC31
						Impressora de targetes	DATACARD	CP60
						Windows 7		
						Impressora làser per PINs i PUKs	HP	Laserjet 2015d
Consell Comarcal del Vallès Oriental	8401	Granollers	P5800010J	ER-042	133	CPU Estació RRA	HP	HP 280 G1
						Monitor Estació RRA	HP	L1750
						Lector de Targetes	Bit4Id	MINILECTOR
						Impressora de targetes	DATACARD	CD800
						Windows 7 64 bits		
						Impressora làser per PINs i PUKs	HP	Laserjet 2015d
Consell Comarcal de l'Anoia	8700	Igualada	P5800006H	ER-043	134	CPU Estació RRA	HP	HP 280 G1
						Monitor Estació RRA	HP	L1740
						Lector de Targetes	Bit4Id	MINILECTOR
						Impressora de targetes	DATACARD	CD800
						Windows 7 64 bits		
						Impressora làser per PINs i PUKs	HP	Laserjet 2015d
Consell Comarcal del Pla d'Urgell	25230	Mollerussa	P7500012E	ER-044	135	CPU Estació RRA	HP	HP 280 G1
						Monitor Estació RRA	HP	L1740
						Lector de Targetes	Bit4Id	MINILECTOR
						Impressora de targetes	DATACARD	CD800
						Windows 7 64 bits		
						Impressora làser per PINs i PUKs	HP	Laserjet 2015d
Ajuntament de Tarragona	43003	Tarragona	P4315000B	ER-045	128	CPU Estació RRA	HP	DC7800 SFF
						Monitor Estació RRA	HP	L1750
						Lector de Targetes	C3PO	LTC-31
						Impressora de targetes	DATACARD	CP60 PLUS
						Windows XP		
						Impressora làser per PINs i PUKs	HP	Laserjet 2015d
Consell Comarcal de la Noguera	25600	Balaguer	P7500005I	ER-046	136	CPU Estació RRA	HP	HP 280 G1
						Monitor Estació RRA	HP	L1750
						Lector de Targetes	Bit4Id	ACR38
						Impressora de targetes	DATACARD	CP60
						Windows 7 64 bits		
						Impressora làser per PINs i PUKs	HP	Laserjet 2015d
Consell comarcal del Berguedà	8600	Berga	P0800015J	ER-047	137	CPU Estació RRA	HP	HP 280 G1
						Monitor Estació RRA	HP	L1750
						Lector de Targetes	Bit4Id	ACR38
						Impressora de targetes	DATACARD	CP60
						Windows 7 64 bits		
						Impressora làser per PINs i PUKs	HP	Laserjet 2015d
Consell comarcal del Baix Empordà	17100	La Bisbal de l'empordà	P6700009A	ER-048	138	CPU Estació RRA	HP	HP 280 G1
						Monitor Estació RRA	HP	L1740
						Lector de Targetes	Bit4Id	LTC31
						Impressora de targetes	DATACARD	CP60
						Windows 7 64 bits		
						Impressora làser per PINs i PUKs	HP	Laserjet 2015d
Consell comarcal del Pallars Jussà	25620	Tremp	P7500014A	ER-049	139	CPU Estació RRA	HP	HP 280 G1
						Monitor Estació RRA	HP	L1750
						Lector de Targetes	Bit4Id	ACR38
						Impressora de targetes	DATACARD	CP60
						Windows 7 64 bits		
						Impressora làser per PINs i PUKs	HP	Laserjet 2015d
Consell comarcal de l'Urgell	25300	Tàrrega	P7500003D	ER-050	140	CPU Estació RRA	HP	HP 280 G1
						Monitor Estació RRA	HP	L1750
						Lector de Targetes	Bit4Id	ACR38
						Impressora de targetes	DATACARD	CD800
						Windows 7 64 bits		
						Impressora làser per PINs i PUKs	HP	Laserjet 2015d
Consell Comarcal del Vallès Occidental	8227	Terrassa	P5800007F	ER-051	141	CPU Estació RRA	HP	HP 280 G1
						Monitor Estació RRA	HP	L1750
						Lector de Targetes	Bit4Id	ACR38
						Impressora de targetes	DATACARD	CD800
						Windows 7 64 bits		
						CPU Estació RRA	HP	DC7800 SFF
Consell Comarcal del Montsià	43870	Amposta	P9300008A	ER-052	143	CPU Estació RRA	HP	HP 280 G1
						Monitor Estació RRA	HP	L1750
						Lector de Targetes	Bit4Id	ACR38
						Impressora de targetes	DATACARD	CD800
						Windows 7 64 bits		
						Impressora làser per PINs i PUKs	HP	Laserjet 2015d
CTTI	8908	Hospitalet de Llobregat	Q5856338H	ER-053	302	CPU Estació RRA	HP	DC7800 SFF
						Monitor Estació RRA	HP	L1750
						Lector de Targetes	Bit4Id	ACR38
						Impressora de targetes	DATACARD	CP60
						Windows 7 32 bits		
						Impressora làser per PINs i PUKs	HP	

Parlament	8003	Barcelona	Q5856081D	ER-054	000	CPU Estació RRA	HP	DC5100/P5 650 SFF
						Monitor Estació RRA	HP	L1702
						Lector de Targetes	C3PO	LTC-31
						Impressora de targetes	DATACARD	ImageCard Select PS
						Impressora làser per PINs i PUKs	HP	Laserjet 2055d
Diputació de Tarragona	43003	Tarragona	P9300002D	ER-055	100	CPU Estació RRA	HP	DC7900 COMPAQ
						Monitor Estació RRA	HP	L1702
						Lector de Targetes	C3PO	LTC-31
						Impressora de targetes	DATACARD	CP40
						Windows Vista 32 bits		
						Impressora làser per PINs i PUKs	HP	Laserjet 2010
Consell Comarcal de l'Alt Empordà	17600	Figueres	P6700008C	ER-056	145	CPU Estació RRA	HP	G280 G1
						Monitor Estació RRA	HP	LE1901W
						Lector de Targetes	C3PO	LTC-31
						Impressora de targetes	DATACARD	CD800
						Windows 7 64 bits		
						CPU Estació RRA	HP	Laserjet 2055d
Consell Comarcal del Garraf	8800	Vilanova i la Geltrú	P5800020I	ER-057	142	CPU Estació RRA	HP	HP 280 G1
						Monitor Estació RRA	HP	L1750
						Lector de Targetes	Bit4Id	ACR38
						Impressora de targetes	DATACARD	CP60
						Windows 7 64 bits		
						Impressora làser per PINs i PUKs	HP	Laserjet 2015d
Ajuntament de Sabadell	8201	Sabadell	P0818600I	ER-059	144	CPU Estació RRA	DELL	Optiplex X755
						Monitor Estació RRA	DELL	
						Lector de Targetes	C3PO	LTC-31
						Impressora de targetes	DATACARD	CP60
						Windows XP		
						Impressora làser per PINs i PUKs	HP	Laserjet 1320n
Conselh Generau d'Aran	25530	Vielha	P7500011G	ER-060	150	CPU Estació RRA	HP	G280 G1
						Monitor Estació RRA	HP	LA1951G
						Lector de Targetes	Bit4id	ACR38
						Impressora de targetes	DATACARD	CP 60 plus
						Windows 7 64 bits		
						Impressora làser per PINs i PUKs	HP	Laserjet 2055d
Consell Comarcal de les Garrigues	25400	Les Borges Blanques	P7500004B	ER-061	149	CPU Estació RRA	HP	G280 G1
						Monitor Estació RRA	HP	LA1951G
						Lector de Targetes	Bit4id	ACR38
						Impressora de targetes	DATACARD	CP 60 plus
						Windows 7 64 bits		
						Impressora làser per PINs i PUKs	HP	Laserjet 2055d
Consell Comercal del Priorat	43730	Falset	P9300009L	ER-062	147	CPU Estació RRA	HP	G280 G1
						Monitor Estació RRA	**HP**	LA1951G
						Lector de Targetes	Bit4id	ACR38
						Impressora de targetes	DATACARD	CP 60 plus
						Windows 7 64 bits		
						Impressora làser per PINs i PUKs	HP	Laserjet 2055d
Consell Comarcal del Solsonès	25280	Solsona	P7500009A	ER-063	151	CPU Estació RRA	HP	G280 G1
						Monitor Estació RRA	HP	LA1951G
						Lector de Targetes	Bit4id	ACR38
						Impressora de targetes	DATACARD	CP 60 plus
						Windows 7 64 bits		
						Impressora làser per PINs i PUKs	HP	Laserjet 2055d
Consell Comarcal de l'Alta Ribagorça	25550	El Pont de Suert	P7500013C	ER-064	146	CPU Estació RRA	HP	DC7900 SFF
						Monitor Estació RRA	HP	LA1951G
						Lector de Targetes	Bit4id	ACR38
						Impressora de targetes	DATACARD	CD800
						Windows 7 64 bits		
						Impressora làser per PINs i PUKs	HP	Laserjet 2055d
Consell Comarcal del Baix Penedès	43700	El vendrell	P9300006E	ER-065	148	CPU Estació RRA	HP	DC7900 SFF
						Monitor Estació RRA	HP	LA1951G
						Lector de Targetes	Bit4id	ACR38
						Impressora de targetes	DATACARD	CP 60 plus
						Windows 7 64 bits		
						Impressora làser per PINs i PUKs	HP	Laserjet 2055d
Consell Comarcal del Bages	8241	Manresa	P5800009B	ER-066	152	CPU Estació RRA	HP	DC7900 SFF
						Monitor Estació RRA	HP	LA1951G
						Lector de Targetes	Bit4id	ACR38
						Impressora de targetes	DATACARD	CP 60 plus
						Windows 7 64 bits		
						Impressora làser per PINs i PUKs	HP	Laserjet 2055d
CATCert LRA PRODUCCIÓ		Barcelona		ER-067		CPU Estació RRA	HP	DC7700 SFF
						Monitor Estació RRA	HP	L1940
						Lector de Targetes	C3PO	LTC-31
						Impressora de targetes	DATACARD	CD800
						Impressora làser per PINs i PUKs	HP	Laserjet 2015d
CESCA (CSUC)	8034	Barcelona		no té ID	000	CPU Estació RRA	HP	D530
						Monitor Estació RRA	Phillips	107511
						Lector de Targetes	Cherry	ACR38
						Impressora de targetes	DATACARD	CP40+
						Impressora làser per PINs i PUKs	HP	LJ P2015d
Consell Comarcal de la Cerdanya	17520	Puigcerdà	P1700016G	ER-068	**153**	CPU Estació RRA	HP	DC7900 SFF
						Monitor Estació RRA	HP	LA1951G
						Lector de Targetes	Bit4id	ACR38
						Impressora de targetes	DATACARD	CP40+
						Windows 7 64 bits		
						Impressora làser per PINs i PUKs	HP	Laserjet 2055d
Agència Catalana de la Protecció de Dades	8018	Barcelona	P5800009B	ER-069	303	CPU Estació RRA	HP	DC7900 SFF
						Monitor Estació RRA	HP	LA1951G
						Lector de Targetes	Bit4id	ACR38
						Impressora de targetes	Fargo	CP60Plus
						Windows 7		
						Impressora làser per PINs i PUKs	HP	Laserjet 2055d
						CPU Estació RRA	HP	G280 G1
						Monitor Estació RRA	HP	LA1951G

Consell Comarcal del Gironès	17003	Girona	P6700003D	ER-070	154	Lector de Targetes	Bit4id	ACR38
						Impressora de targetes	Datacard	CD800
						Windows 7 64 bits		
						Impressora làser per PINs i PUKs	HP	Laserjet 2055d
Agjuntament de Cerdanyola del Vallès	8290	Cerdanyola del Vallès	P0826600I	ER-071	155	CPU Estació RRA	HP	DC7900 SFF
						Monitor Estació RRA	HP	LA1951G
						Lector de Targetes	Bit4id	ACR38
						Impressora de targetes	Datacard	CP40+
						Windows 7		
						Impressora làser per PINs i PUKs	HP	Laserjet 2055d
Ajuntament de Mataró	8006	Mataró	P0812000H	ER-072	156	CPU Estació RRA	HP	DC7900 SFF
						Monitor Estació RRA	HP	LA1951G
						Lector de Targetes	Bit4id	ACR38
						Impressora de targetes	Datacard	CP40+
						Windows 7 64 bits		
						Impressora làser per PINs i PUKs	HP	Laserjet 2055d
Ajuntament de Cornellà de Llobregat	8940	Cornellà de Llobregat	P0807200A	ER-073	157	CPU Estació RRA	HP	DC7900 SFF
						Monitor Estació RRA	HP	LA1951G
						Lector de Targetes	Bit4id	ACR38
						Impressora de targetes	Datacard	CP60
						Windows Vista 32 bits		
						Impressora làser per PINs i PUKs	HP	Laserjet 2055d
Departament d'Agricultura	8007	Barcelona	S0811001G	ER-074	304	CPU Estació RRA	HP	DC7900
						Monitor Estació RRA	HP	LE1901W
						Lector de Targetes	Bit4id	ACR38
						Impressora de targetes	Datacard	CP40+
						Windows Vista 32 bits		
						Impressora làser per PINs i PUKs	HP	Laserjet 2055d
Consell Comarcal del Baix Llobregat	08890	Sant Feliu de Llobregat	P5800011H	ER-075	158	CPU Estació RRA	HP	Compaq dc7900
						Monitor Estació RRA	HP	LE 1901W
						Lector de Targetes	Bit4id	ACR38
						Impressora de targetes	DATACARD	CP40 PLUS
						Windows 7 64 bits		
						Impressora làser per PINs i PUKs	HP	Laserjet P2055d
FirmaProfesional	8173	Sant Cugat del Vallès		ER-076	0	CPU Estació RRA	HP	Compaq 8000 ELITE
						Monitor Estació RRA		
						Lector de Targetes		
						Impressora de targetes	Datacard	CP60
						Impressora làser per PINs i PUKs	HP	Laserjet 2055d
FirmaProfesional	8173	Sant Cugat del Vallès		ER-077	0	CPU Estació RRA	HP	Compaq 8000 ELITE
						Monitor Estació RRA	HP	
						Lector de Targetes		
						Impressora de targetes	Datacard	CD800
						Impressora làser per PINs i PUKs		
FirmaProfesional	8173	Sant Cugat del Vallès		ER-078	0	CPU Estació RRA	HP	Compaq 8000 ELITE
						Monitor Estació RRA	HP	LE1901w
						Lector de Targetes		
						Impressora de targetes	Datacard	CD800
						Impressora làser per PINs i PUKs		
Consell Comarcal del Moianès	8180	Moià	P0800317J	ER-079	0	CPU Estació RRA	HP	G280 G1
						Monitor Estació RRA	HP	LE1901w
						Lector de Targetes		
						Impressora de targetes	Datacard	CD800