

PLEC DE PRESCRIPCIONS TÈCNIQUES PARTICULARS PER REALITZAR EL DESENVOLUPAMENT I EL SUPORT A LA POSADA EN MARXA DE PSIS 9.0

Número d'expedient: AOC-2023-44

ÍNDEX DE CLÀUSULES I ANNEXOS

1	OBJECTE DEL CONTRACTE.....	4
2	OBJECTIUS DEL PROJECTE.....	4
3	DESCRIPCIÓ DEL SERVEI ACTUAL	4
3.1	SITUACIÓ ACTUAL	4
3.2	ARQUITECTURA ACTUAL DE L'ENTORN PRODUCTIU (PSIS 6.0)	5
3.3	DEFINICIÓ DE L'ARQUITECTURA DE PSIS 8.0	5
4	DESENVOLUPAMENT I SUPORT A LA POSADA EN MARXA DE PSIS 9.0.....	5
4.1	ABAST I DURADA	5
4.2	DESENVOLUPAMENTS.....	5
4.2.1	<i>Migració de la JVM a la versió estable més recent.....</i>	<i>6</i>
4.2.2	<i>Migració de les llibreries de Spring Framework.....</i>	<i>6</i>
4.2.3	<i>Migració de les llibreries de BouncyCastle.....</i>	<i>7</i>
4.2.4	<i>Migració de les llibreries de Apache Santuario.....</i>	<i>8</i>
4.2.5	<i>Migració de les llibreries de Hibernate</i>	<i>8</i>
4.2.6	<i>Redis</i>	<i>9</i>
4.2.7	<i>Refactoring de la consola web d'administració</i>	<i>10</i>
4.2.8	<i>Servidor web lleuger</i>	<i>10</i>
4.2.9	<i>Estudi de refactoring de l'arquitectura de codi.....</i>	<i>11</i>
4.3	SUPORT A LA POSADA EN MARXA EN PREPRODUCCIÓ I PRODUCCIÓ.....	11
4.3.1	<i>Migració de Oracle a AWS Aurora Serverless V2 (PostgreSQL compatible)</i>	<i>11</i>
4.3.1.1	<i>Preproducció.....</i>	<i>12</i>
4.3.1.2	<i>Producció</i>	<i>13</i>
4.4	DEVSECOPS	15
4.5	EQUIP DE PROJECTE.....	15
4.6	COORDINACIÓ AMB LA OFICINA TÈCNICA DE MANTENIMENT EVOLUTIU I CORRECTIU	16
4.7	REQUERIMENTS FUNCIONALS	16
4.8	REQUERIMENTS TÈCNICS	17
4.8.1	<i>Infraestructura necessària per dur a terme el desenvolupament del projecte</i>	<i>17</i>
4.8.2	<i>Dimensionament.....</i>	<i>17</i>
4.8.3	<i>Codi font i propietat intel·lectual.....</i>	<i>19</i>
4.8.4	<i>Tests unitaris i proves d'integració</i>	<i>19</i>
4.8.5	<i>Tests de rendiment</i>	<i>20</i>
4.9	REQUERIMENTS LEGALS	20
4.10	REQUERIMENTS DE SEGURETAT	20
4.10.1	<i>Mesures de seguretat que ha d'incorporar PSIS 9.0 com a solució</i>	<i>20</i>

4.10.2	<i>Mesures de seguretat a complir per part de l'adjudicatari</i>	21
4.10.2.1	Certificacions de seguretat	21
4.10.2.2	Control d'accés al sistema	21
4.10.2.3	Control de personal	21
4.10.2.4	Protecció de la informació	21
4.10.2.5	Protecció dels suports.....	22
4.11	REQUERIMENTS DE PROTECCIÓ DE DADES	22
4.12	PLA DE DEVOLUCIÓ DEL SERVEI	22
4.13	CONDICIONS D'EXECUCIÓ	23
4.13.1	<i>Obligacions bàsiques</i>	23
4.13.2	<i>Eines de control</i>	23
4.13.3	<i>Normativa aplicable</i>	24
4.14	MODEL DE RELACIÓ.....	24
5	ANNEXOS	25

1 Objecte del contracte

L'objecte del present plec és fixar les prescripcions tècniques particulars que regiran la contractació del desenvolupament i el suport a la posada en marxa de PSIS 9.0 (Plataforma de Serveis d'Identificació i Signatura) del Consorci AOC.

L'objectiu és continuar en la línia de modernització tecnològica de PSIS per tal de garantir la continuïtat del servei en un entorn de consum creixent. El volum actual d'operacions en PSIS és del voltant de 28 milions d'operacions mensuals amb pics de fins a més de 32 milions d'operacions mensuals.

2 Objectius del projecte

L'objectiu és avançar en la modernització de la solució tecnològica actual, desplegada al núvol, per fer ús dels avantatges que aporten les noves tecnologies, per donar solució a les necessitats futures que es preveu que el servei tindrà a mig/llarg termini.

Aquest projecte inclourà:

- Desenvolupament de la solució.
- Tests unitaris.
- Tests funcionals.
- Tests de rendiment.
- Tests de seguretat.
- Realitzar tasques associades a la posada en marxa del servei als entorns de desenvolupament, preproducció i producció.

3 Descripció del servei actual

3.1 Situació actual

El Consorci AOC ofereix a les administracions públiques catalanes el servei de validació. PSIS és la plataforma tecnològica des d'on es presta el servei de validació. El servei de validació comprèn principalment la validació de certificats i la validació i completat o preservació de signatures digitals. També permet la creació i validació de segells de temps i la creació de signatures digitals de forma segura i desatesa.

El servei de validació (en endavant PSIS) és consumit per tots els ens que formen part de l'administració pública catalana que disposen d'aplicacions informàtiques on es fa ús de certificats i signatures digitals, per tal de dotar de seguretat als processos d'identificació i tractament de documents signats. PSIS és un servei transversal que es consumeix per pràcticament la totalitat dels serveis del Consorci AOC, així com per la resta dels ens de l'administració pública catalana. Degut a aquesta transversalitat, és el servei amb més consum del Consorci AOC: L'any 2022 el servei va processar més de 300 milions d'operacions, que representa un increment d'uns 50 milions d'operacions respecte a 2021. El creixement de consum en la resta de serveis es tradueix també en un increment del consum de PSIS.

La solució tecnològica actual, PSIS 8.0, està desenvolupada pel seu desplegament al cloud en Amazon Web Services (en endavant AWS). Actualment està desplegada en AWS només a l'entorn de desenvolupament. Els entorns de preproducció i producció encara els tenim en modalitat on-premises, amb la versió 6.0. PSIS 6.0 és doncs la modalitat on-premises; PSIS 7.0 va ser una versió intermitja que no vam arribar a desplegar als entorns de preproducció i producció, i que incloïa com a canvi principal el desplegament en Kubernetes. I PSIS 8.0 és Kubernetes desplegat al Cloud de AWS amb integració amb serveis de AWS.

Està previst desplegar la versió 8.0 en preproducció i producció al segon semestre de 2023.

La solució PSIS 8.0 és totalment funcional. Però cal actualitzar-la i modernitzar les tecnologies emprades. PSIS 9.0 es desenvoluparà a partir de PSIS 8.0.

3.2 Arquitectura actual de l'entorn productiu (PSIS 6.0)

Per a més informació consulteu el document *Annex2_Arquitectura_PSIS6.0.pdf* (per descarregar aneu al punt 5 Annexos).

3.3 Definició de l'arquitectura de PSIS 8.0

Per a més informació consulteu el document *Annex3_AOC_Definició_Arquitectura_PSIS_8.0.pdf* (per descarregar aneu al punt 5 Annexos).

4 Desenvolupament i suport a la posada en marxa de PSIS 9.0

Descripció dels serveis a prestar per part de l'adjudicatari.

4.1 Abast i durada

L'abast del projecte comprèn el desenvolupament i el suport a la posada en marxa de PSIS 9.0.

La definició final del desenvolupament serà consensuada conjuntament entre l'adjudicatari i el Consorci AOC.

- En aquest contracte es continuarà amb el desenvolupament de la solució de PSIS al núvol d'AWS. PSIS ja està desplegada en AWS, i els evolutius que es duren a terme en el present contracte estan enfocats a la modernització del codi font i l'arquitectura (si s'escau).
- El Consorci AOC proporciona l'espai necessari a AWS per a l'entorn de desenvolupament. La infraestructura i espai a AWS dels entorns de preproducció i producció seran proporcionats pel Consorci AOC al llarg del 2023.
- Construcció i desenvolupament de la solució en l'entorn de desenvolupament.
- S'inclou el suport a la instal·lació i al desplegament del servei en els sistemes tècnics del Consorci AOC (entorns de preproducció i producció).
- Documentació, creació dels processos i formació detallades de cadascuna d'aquestes activitats.
- L'execució de les tasques encomanades s'haurà de dur a terme a les instal·lacions de l'adjudicatari. És possible que en alguna ocasió sigui necessari el desplaçament d'algun dels membres de l'equip a les instal·lacions del Consorci AOC.

La prestació del servei començarà el 01/07/2023 (o en la data de formalització del contracte) i finalitzarà el 31/12/2024.

4.2 Desenvolupaments

A continuació descrivim les tasques de desenvolupament que caldrà fer sobre la solució de PSIS desplegada en AWS.

4.2.1 Migració de la JVM a la versió estable més recent

Actualment PSIS està funcionant amb la versió de java 1.8.0_291. Java 8 ha assolit el final de les actualitzacions públiques, és a dir, que no es publicaran noves versions sobre Java 8. Oracle no ofereix servei de suport gratuït per les versions Java 7 i Java 8.

A data de gener de 2023, Java 17 LTS és l'última versió amb suport a llarg termini per a la plataforma Java SE.

Els binaris JDK 19 i JDK 17 es distribueixen de manera gratuïta i es poden fer servir en entorns productius, sense cap cost, d'acord a la política de *No-Fee Terms and Conditions* d'Oracle. JDK 19 rebrà actualitzacions d'acord amb aquestes condicions, fins al març de 2023, quan serà substituïda per JDK 20. JDK 17 rebrà actualitzacions segons aquestes condicions, com a mínim fins al setembre de 2024.

La versió de Java més actual doncs a data de gener de 2023 és la versió 19, i serà substituïda per la versió 20 al març de 2023. Per tal de poder gaudir de suport gratuït i sobretot, per tal de poder aprofitar les millores que ens ofereixen les versions que s'han anat introduint des de la versió 8 en endavant (com la resolució de bugs, de vulnerabilitats de seguretat, etc.), és important actualitzar el codi de PSIS a la versió estable més actual possible.

En la següent pàgina web Oracle informa de les millores i correccions introduïdes en les diferents releases:

<https://www.oracle.com/java/technologies/javase/jdk-relnotes-index.html>

Tasques a realitzar per part de l'adjudicatari:

- Escollir la versió més adient de la JVM, tenint en compte les necessitats de les migracions de les llibreries de Spring (4.2.2), BouncyCastle (4.2.3) i Apache Santuario (4.2.4), i Hibernate (4.2.5).

4.2.2 Migració de les llibreries de Spring Framework

Actualment PSIS fa servir la versió 5.1.7 del framework de Spring. La versió més actual d'aquestes llibreries és la versió 6.0.x.

Les versions que tenen suport oficial actualment (gener de 2023) són:

- 6.0.x és la línia de producció principal a partir de novembre de 2022. Aquesta nova generació del framework inclou una línia de base JDK 17 i Jakarta EE 9.
- 5.3.x és la branca final de la cinquena generació, amb suport a llarg termini proporcionat per a JDK 8, JDK 11, JDK 17 i Java EE 8.
- 4.3.x va assolir el seu EOL oficial (final de vida útil) el 31 de desembre de 2020. No hi ha previst cap més pegat de manteniment i seguretat en aquesta línia.
- 3.2.x va assolir el seu EOL oficial (final de vida útil) el 31 de desembre de 2016. No hi ha previst cap pegat de seguretat i manteniment en aquesta línia.

Les versions de la JVM suportades són:

- Spring Framework 6.0.x: JDK 17-21
- Spring Framework 5.3.x: JDK 8-19

Tasques a realitzar per part de l'adjudicatari:

- Estudi comparatiu de migració a les versions 5.3 i 6.0.
- Proposta de disseny dels canvis que impliqui en PSIS la versió escollida.
- Proves de rendiment per garantir que mantenim, com a mínim, el mateix rendiment que amb la versió actual.
- Anàlisi dels canvis a realitzar: Revisió dels objectius del projecte i consens amb el Consorci AOC sobre com assolir-los.

4.2.3 Migració de les llibreries de BouncyCastle

Les API Crypto de Bouncy Castle per a Java consisteixen en el següent:

- Una API de criptografia lleugera.
- Un proveïdor de Java Cryptography Extension (JCE) i Java Cryptography Architecture (JCA).
- Un proveïdor per Java Secure Socket Extension (JSSE).
- Implementació *clean room* de la JCE 1.2.1.
- Una biblioteca per llegir i escriure objectes ASN.1 codificats.
- API lleugeres per a TLS (RFC 2246, RFC 4346) i DTLS (RFC 6347/RFC 4347).
- Generadors de certificats X.509 versió 1 i versió 3, CRL versió 2 i fitxers PKCS12.
- Generadors de certificats d'atributs X.509 versió 2.
- Generadors/processadors per a S/MIME i CMS (PKCS7/RFC 3852).
- Generadors/processadors per a OCSP (RFC 2560).
- Generadors/processadors per a TSP (RFC 3161 i RFC 5544).
- Generadors/processadors per a CMP i CRMF (RFC 4210 i RFC 4211).
- Generadors/processadors per a OpenPGP (RFC 4880).
- Generadors/processadors per a control d'accés estès (EAC: *Extended Access Control*).
- Generadors/processadors per a validació de dades i servidor de certificació (DVCS: *Data Validation and Certification Server*) - RFC 3029.
- Generadors/processadors per a l'autenticació d'entitats amb nom basat en DNS (DANE: *DNS-based Authentication of Named Entities*).
- Generadors/processadors per a la inscripció RFC 7030 a través del transport segur (EST: *Enrollment over Secure Transport*).
- Versions jar signades adequades per a JDK 1.4-1.8 i Sun JCE.

PSIS fa servir aquesta llibreria per validar certificats, per crear, validar i completar signatures en format ASN.1, i per crear i validar segells de temps en format ASN.1, etc.

A la taula següent tenim la versió de les llibreries BouncyCastle que fa servir actualment PSIS, en paral·lel a la versió més recent a gener de 2023 publicada per JDK 1.8 i superiors:

Descripció del paquet	Llibreria PSIS	Data	Última versió per JDK 1.8 i superiors	Data
PROVIDER	bcprov-jdk15on-1.49.jar	31/maig/2013	bcprov-jdk18on-172.jar	25/setembre/2022
PKIX/CMS/EAC/PKCS/OCSP/TSP/OPENSSL	bcpkix-jdk15on-1.49.jar	31/maig/2013	bcpkix-jdk18on-172.jar	25/setembre/2022
SMIME	bcmail-jdk15on-1.49.jar	31/maig/2013	bcmail-jdk18on-172.jar	25/setembre/2022

En la següent pàgina web tenim informació sobre les diferents versions que s'han publicat de les llibreries de BouncyCastle per Java:

https://www.bouncycastle.org/latest_releases.html

Cal dir que la versió més actual de BouncyCastle no és compatible amb les versions anteriors. Per tant, actualitzar-la implica refer el codi que fa servir les APIs de BouncyCastle.

Tasques a realitzar per part de l'adjudicatari:

- Refactoring del codi de PSIS per fer servir la versió més actual de les llibreries.

4.2.4 Migració de les llibreries de Apache Santuario

El projecte Apache Santuario té com a objectiu proporcionar la implementació dels estàndards de seguretat primaris per a XML:

- Sintaxi i processament de la signatura XML
- Sintaxi i processament de xifrat XML.

La llibreria que proporciona les funcionalitats anteriors per a Java és Apache XML Security per Java. Aquesta llibreria inclou una implementació avançada de signatura digital i xifrat. També inclou l'API estàndard JSR 105 (Java XML Digital Signature).

PSIS fa servir aquesta llibreria per crear, validar i completar signatures, i validar segells de temps en format XML.

A la taula següent tenim la versió de la llibreria Apache XML Security que fa servir actualment PSIS, així com al versió més recent publicada per Java:

Descripció del paquet	Llibreria PSIS	Data	Última versió per JDK 1.8 i superiors	Data
Apache XML Security	xmlsec-2.0.6.jar	12/abril/2015	xmlsec-3.0.1.jar	12/setembre/2022

En la següent pàgina web tenim informació sobre les diferents versions que s'han publicat de la llibreria de XML Security per Java:

<https://santuario.apache.org/javareleasenotes.html>

Cal tenir en compte que aquesta llibreria està modificada pel seu ús en PSIS, per suplir mancances que es van trobar originalment durant el desenvolupament inicial de PSIS. Caldrà veure si les darreres versions cobreixen aquests mancances o si també cal modificar el codi font.

Tasques a realitzar per part de l'adjudicatari:

- Refactoring del codi de PSIS per fer servir la versió més actual de les llibreries.

4.2.5 Migració de les llibreries de Hibernate

Hibernate és una eina de mapeig objecte-relacional (ORM) per a la plataforma Java, que facilita el mapeig d'atributs entre una base de dades relacional tradicional i el model d'objectes d'una aplicació, mitjançant arxius declaratius (XML) o anotacions als beans de les entitats que permeten establir aquestes relacions. Hibernate és també una implementació de l'especificació Java Persistence API (JPA).

Hibernate és programari lliure, distribuït sota els termes de la llicència LGPL V2.1.

L'API Java Persistence (JPA), el 2019 rebatejada a Jakarta Persistence (després de que Java EE passés a ser codi obert ofert per Oracle i aquest donés els drets a Eclipse Foundation, estaven legalment obligats a canviar el nom de Java, ja que Oracle té els drets sobre la marca Java), és una especificació d'interfície de programació d'aplicacions Java que descriu la gestió de dades relacionals en aplicacions que utilitzen la plataforma Java, Standard Edition i Java Platform, Enterprise Edition/Jakarta EE.

PSIS utilitza actualment la versió 2.1 de la JPA del Hibernate ORM 5.0. Però Hibernate ORM 5.0 ha arribat al final del seu cicle de vida. Caldria actualitzar a una versió recent de les llibreries.

A la següent URL tenim informació sobre les diferents versions. A data de gener de 2023 la versió estable més actual és la 6.1.

<https://hibernate.org/orm/releases/>

A la taula següent es mostra la matriu de compatibilitat entre les versions de java, i JPA/Jakarta Persistence, més actuals:

Hibernate ORM	6.2	6.1	5.6
Java	11, 17 o 18	11, 17 o 18	8, 11, 17 o 18
JPA	N/A	N/A	2.2
Jakarta Persistence	3.1	3.1 i 3.0	3.0

Tasques a realitzar per part de l'adjudicatari:

- Estudi dels canvis que suposa la migració a la versió 3.1 (o la més nova a l'adjudicació d'aquest concurs).
- Proposta de disseny dels canvis.
- Proves de rendiment per garantir que mantenim, com a mínim, el mateix rendiment que amb la versió actual.
- Anàlisi dels canvis a realitzar: Revisió dels objectius del projecte i consens amb el Consorci AOC sobre com assolir-los.

4.2.6 Redis

La configuració de PSIS actualment es troba definida en uns arxius XML que es carreguen en la base de dades. Quan parlem de configuració estem fent referència a la configuració interna de tots els serveis que conformen PSIS. Un desplegament en PSIS pot ser un desplegament de codi, un desplegament de configuració, o ambdós.

L'aplicació PSIS consumeix la configuració de la base de dades, i la carrega en la caché del servidor d'aplicacions.

Amb aquest desenvolupament és pretén migrar la configuració de la base de dades actual (AWS Aurora PostgreSQL) a Redis, i consumir-la directament des de Redis o carregar-la en la caché del servidor d'aplicacions (dependrà del rendiment i/o els costos d'explotació en AWS).

Donat que PSIS 8.0 està desplegat en AWS, la migració es faria cap al servei Amazon ElastiCache for Redis. Amazon ElastiCache for Redis és un magatzem de dades en memòria increïblement ràpid que ofereix una latència inferior a un mil·lisegon per a aplicacions en temps real a escala d'Internet. Creat sobre Redis de codi obert i compatible amb les API de Redis, ElastiCache per a Redis es pot fer servir amb clients de Redis i utilitza el format de dades de Redis obert per a l'emmagatzematge. Això ens permetrà un desenvolupament lo més agnòstic possible del cloud en que estigui desplegat PSIS.

ElastiCache proporciona la capacitat de crear i administrar usuaris i grups d'usuaris que es poden utilitzar per configurar el control d'accés basat en rols (RBAC) per a les comandes de Redis. És possible utilitzar AWS Identity and Access Management (IAM) per connectar-se a ElastiCache per a Redis amb identitats de l'IAM. Redis compleix els requisits de PCI i HIPAA, està autoritzat per FedRAMP i ofereix xifrat en trànsit i en repòs (inclosa la CMK administrada per l'usuari emmagatzemada a AWS KMS), a més d'AUTH de Redis per a les comunicacions segures entre nodes per protegir informació confidencial, com ara la informació d'identificació personal (PII).

Els objectius de la migració són:

- Poder disposar simultàniament de més d'una versió de la configuració. Això ens permetria poder canviar de versió simplement apuntat a una o altra versió de la configuració.
- Agilitzar els desplegaments. Actualment un canvi de configuració implica tall de servei. Volem que el canvi de configuració es pugui fer en calent.
- Millorar el rendiment.

Tasques a realitzar per part de l'adjudicatari:

- Proposta d'adaptació dels arxius XML de configuració actual als requerits per la migració a Redis.

- Proposta de disseny dels canvis en PSIS per tal de consumir la configuració des de Redis.
- Proves de rendiment per garantir que mantenim, com a mínim, el mateix rendiment que amb el model actual.
- Anàlisi dels canvis a realitzar: Revisió dels objectius del projecte i consens amb el Consorci AOC sobre com assolir-los.

4.2.7 Refactoring de la consola web d'administració

Actualment PSIS disposa de dues consoles:

- Una consola web que permet administrar la configuració dels serveis:
 - Càrrega de configuració.
 - Càrrega/eliminació de certificats al Truststore.
 - Una consola java que proporciona les següents funcionalitats:
 - Càrrega de bindings o claus criptogràfiques.
 - Càrrega de polítiques de signatura.
 - Càrrega de CRLs en base de dades.
- Nova funcionalitat que haurà d'incloure (actualment no es proporciona aquesta funcionalitat):
- Càrrega de respostes OCSP en base de dades.

Lo que volem és unificar en una sola consola web totes aquestes funcionalitats. Aquesta nova consola web substituiria a les dues actuals.

Tasques a realitzar per part de l'adjudicatari:

- Proposta de disseny tècnic de la nova consola web.
- Proposta de disseny de les diferents pantalles.
- Estudi de viabilitat i cost de desplegament/exploitació en EKS vs EC2 de AWS.
- Anàlisi dels canvis a realitzar: Revisió dels objectius del projecte i consens amb el Consorci AOC sobre com assolir-los.

4.2.8 Servidor web lleuger

Actualment PSIS està desplegat en Kubernetes en contenidors sobre un servidor d'aplicacions Java EE. La idea és adaptar l'aplicació pel seu desplegament en un servidor web lo més lleuger possible i que al mateix temps proporcionï el major rendiment possible.

Entre els servidors Java EE open source més populars, tenim:

- Apache Tomcat:
 - Proporciona un entorn flexible amb eines de personalització integrades.
 - Utilitza codi lleuger que permet un desplegament i una càrrega més ràpids de les aplicacions.
 - És una plataforma relativament més estable que altres servidors d'aplicacions Java EE.
- Jetty
 - Ofereix flexibilitat perquè es pot utilitzar com a nivell web per a les piles de servidors d'aplicacions Java totals i parcials.
 - Gestiona fins a 10.000 sol·licituds, de manera que és extremadament ràpid i flexible.
 - És altament escalable gràcies a un disseny de memòria de servlet petit.
- Glassfish
 - Proporciona un suport òptim per a Enterprise JavaBeans, Java Server Faces, JMS, JPA i molts altres.
 - Fàcil de desplegar codis Java a causa del seu disseny lleuger.

- Permet crear programari empresarial portàtil i escalable, i integrar-lo amb sistemes legacy.
- JBoss Enterprise Application Platform
 - Més fàcil accés a les eines de codi obert gràcies al suport de Red Hat.
 - Compleix amb les especificacions Java EE 7.
 - Hi ha serveis web, piles i arquitectures al núvol.
 - Les funcions d'automatització faciliten la gestió.

Tasques a realitzar per part de l'adjudicatari:

- Estudi sobre la idoneïtat per a PSIS dels diferents servidors d'aplicacions, així com de la viabilitat de migració des del servidor d'aplicacions actual. Comparativa entre el servidor d'aplicacions actual i l'escollit per dur a terme la migració.
- Anàlisi dels canvis a realitzar: Revisió dels objectius del projecte i consens amb el Consorci AOC sobre com assolir-los.

4.2.9 Estudi de refactoring de l'arquitectura de codi

Estudi de la viabilitat tècnica d'alternatives de rearquitectura de l'aplicació, que ofereixin més avantatges i puguin ser incloses en l'abast definit pels objectius. Disseny tècnic detallat amb èmfasi en diagrames de desplegament, i impacte en components actuals. Es podran considerar unes alternatives principals, o combinació d'elles, amb la intenció de seleccionar aquella(es) que impliqui(n) major benefici en rendiment i reducció de costos d'explotació i infraestructura. Alternatives a considerar:

- **CaaS de Web Server** (*Container as a Service* de Web Server).
És la opció més senzilla, però potser la menys eficient.
- **CaaS amb Spring Boot** (*Container as a Service* amb migració a Spring Boot)
Spring és un framework de desenvolupament d'aplicacions i contenidor d'inversió de control, de codi obert, per a la plataforma Java.
- **CaaS amb GraalVM i Quarkus**
GraalVM: Motor d'execució d'alt rendiment, dissenyat per accelerar l'execució d'aplicacions escrites en Java i altres llenguatges JVM.
Quarkus: Framework Java nadiu de Kubernetes dissenyat per OpenJDK HotSpot i GraalVM. Comparativament a d'altres frameworks, com per exemple Spring, ofereix menor impacte en memòria i reducció considerable del temps d'arrencada.
- **FaaS amb Spring Boot** (*Function as a Service* amb Spring Boot)
En aquest cas cal assegurar la portabilitat de la solució a un cloud diferent.
Exemple: AmazonWS Lambda.
- **FaaS amb Spring Cloud Function** (*Function as a Service* amb Spring Cloud Function)
Spring Cloud Function és un component de l'stack d'Spring que permet fer aplicacions Serverless agnòstiques al lloc on es desplegaran.

4.3 Suport a la posada en marxa en reproducció i producció

4.3.1 Migració de Oracle a AWS Aurora Serverless V2 (PostgreSQL compatible)

Les dades dels entorns productius actuals (primari i secundari) es troben en una base de dades **Oracle 12c**. En la versió de PSIS al núvol, la base de dades Oracle ha sigut substituïda per **AWS Aurora Serverless V2** compatible amb PostgreSQL.

L'esquema de dades ja el tenim definit a Aurora. Cal migrar les dades, les quals caldrà convertir durant el procés de migració al nou esquema compatible amb PostgreSQL.

A l'entorn de desenvolupament ja hem migrat les dades necessàries.

Les dades en Oracle que cal migrar a Aurora Serverless V2 de AWS són dades que contenen les llistes de revocació de certificats (en endavant CRL, de *Certificate Revocation Lists*) i respostes OCSP (*Online Certificate Status Protocol*). Són dades que PSIS guarda després de fer-les servir per la validació de certificats. Cada cop que PSIS valida un certificat, guarda en base de dades la CRL (si no existeix prèviament) o resposta OCSP corresponent. No només com a evidència del procés de validació, sinó també per reutilitzar-la mentre duri el temps de confiança (1 hora per CRLs, i 6 minuts i 40 segons per les respostes OCSP), així com per poder recuperar-la en un futur per la validació de signatures amb segell de temps.

Les CRLs i respostes OCSP estan historificades anualment, distribuïdes en diferents taules en funció de l'any.

4.3.1.1 Preproducció

L'entorn de preproducció és únic, i només tenim una base de dades. El volum total d'informació de revocació fins a desembre de 2022 inclòs és d'uns **11 GB**.

A l'entorn de preproducció tenim dades des de l'any 2009.

Any	Volum en MB
2009	5,25
2010	55,31
2011	69,06
2012	115,81
2013	45,94
2014	178,00
2015	244,75
2016	459,13
2017	505,06
2018	953,13
2019	1.133,13
2020	1.371,00
2021	3.776,00
2022	2.469,63
TOTAL	11.381,19 MB

En relació al número de CRLs i OCSPs, tenim, a data de desembre de 2022, uns totals de **més de 200.000 CRLs** i **més de 2 milions de respostes OCSP**, distribuïdes per any segons la taula següent:

Any	CRLs	Respostes OCSP
2009	4.801	584
2010	15.259	12.890
2011	43.534	9.416
2012	8.688	70.098
2013	10.891	56.171

2014	11.641	98.889
2015	8.450	108.902
2016	11.764	116.456
2017	11.020	109.792
2018	11.406	199.337
2019	11.756	258.003
2020	10.785	272.020
2021	29.571	487.064
2022	16.442	344.551
TOTAL	206.008	2.144.173

4.3.1.2 Producció

L'entorn productiu s'ofereix en alta disponibilitat i consta de 2 entorns, anomenats primari i secundari. Estan dimensionats de la mateixa manera, i el servei es pot oferir des de qualsevol dels dos en tot moment. Mai però s'ofereix des d'ambdós a l'hora. Anomenem "primari" a l'entorn des del qual s'està oferint el servei de manera preferent en un moment donat.

Als entorns productius però el volum de dades és molt superior que a l'entorn de preproducció, i a més necessitem poder realitzar la migració en calent i en un temps lo més reduït possible.

El volum de dades és important. Estem parlant de 2 entorns productius, cadascun d'ells amb un volum de dades considerable.

Als entorns de producció tenim dades des de l'any 2006.

El volum de dades que tenim fins a desembre de 2022 inclòs és d'uns **660 GB**, repartits per entorn productiu segons la taula següent:

Entorn productiu	Volum de dades de revocació
PSIS 1	420 GB
PSIS 2	243 GB
TOTAL	663 GB

Les dades amb informació de revocació es distribueixen anualment i per entorn productiu de la següent manera:

Any	Volum en MB		
	PSIS 1	PSIS 2	Total MB
2006	1,88	1,94	3,81
2007	6,88	8,94	15,81
2008	21,56	22,44	44,00
2009	56,88	55,56	112,44
2010	1.803,06	1.862,75	3.665,81
2011	1.536,06	1.517,56	3.053,63
2012	2.031,81	1.156,06	3.187,88
2013	3.198,63	32,75	3.231,38
2014	5.645,75	169,44	5.815,19
2015	8.710,81	310,69	9.021,50

2016	16.437,06	575,31	17.012,38
2017	30.460,06	1.132,25	31.592,31
2018	57.233,06	896,63	58.129,69
2019	53.138,06	17.282,06	70.420,13
2020	18.831,06	101.338,06	120.169,13
2021	33.489,06	114.507,00	147.996,06
2022	188.035,00	2.305,75	190.340,75
TOTAL	420.636,69 MB	243.175,19 MB	663.811,88 MB

En relació al número de CRLs i OCSPs, tenim, a data de desembre de 2022, uns totals de **3,2 milions de CRLs** i **116,2 milions de respostes OCSP**:

Entorn productiu	Nº CRLs	Nº OCSPs
PSIS 1	1,7 milions	78,3 milions
PSIS 2	1,5 milions	37,9 milions
TOTAL	3,2 milions	116,2 milions

Distribuïts per entorn productiu i any segons la taula següent:

Any	CRLs			Respostes OCSP		
	PSIS 1	PSIS 2	Total	PSIS 1	PSIS 2	Total
2006	1.274	1.274	2.548	24	24	48
2007	6.420	6.483	12.903	563	560	1.123
2008	7.334	7.395	14.729	23.131	23.106	46.237
2009	9.385	9.443	18.828	86.520	86.514	173.034
2010	138.382	138.486	276.868	566.465	566.418	1.132.883
2011	107.054	107.479	214.533	519.029	518.089	1.037.118
2012	28.882	24.140	53.022	712.397	428.354	1.140.751
2013	20.571	1.813	22.384	1.132.445	51.936	1.184.381
2014	25.620	5.212	30.832	1.943.143	93.722	2.036.865
2015	28.370	4.784	33.154	3.317.155	136.933	3.454.088
2016	55.178	3.554	58.732	5.665.178	128.401	5.793.579
2017	89.938	5.792	95.730	8.054.060	299.383	8.353.443
2018	64.765	3.773	68.538	8.208.180	134.289	8.342.469
2019	302.456	145.671	448.127	7.561.047	2.464.170	10.025.217
2020	101.686	503.619	605.305	2.966.163	15.629.074	18.595.237
2021	123.618	521.260	644.878	5.361.444	17.008.281	22.369.725
2022	627.900	20.681	648.581	32.223.855	348.213	32.572.068
TOTAL	1.738.833	1.510.859	3.249.692	78.340.799	37.917.467	116.258.266

És molt important tenir en compte que una mateixa CRL pot estar present en ambdós entorns. Les CRLs caldrà consolidar-les tenint en compte que han de ser úniques.

En el cas de les respostes OCSPs, per la seva natura, són úniques. Tanmateix és possible que una mateixa resposta OCSP estigui present en ambdós entorns, perquè l'entorn secundari es va

crear inicialment sobre una còpia de les dades de l'entorn primari. Per tant, també haurem de tenir en compte que aquestes dades poden estar presents en ambdós entorns i que caldrà consolidar-les eliminant duplicats i preservant la unicitat.

Donat que es tracta d'un entorn productiu, les dades de l'any en curs s'hauran de migrar en calent. I fins al moment en que PSIS en producció s'ofereixi des de AWS, caldrà anar migrant les noves dades que es vagin introduint en aquestes taules fruit del funcionament normal del servei. En aquest cas això només aplicaria a l'entorn productiu que estigui donant servei en aquell moment.

Com a exemple de migració fent servir les eines de AWS, en la següent URL s'exposa una estratègia de migració des d'Oracle cap a Aurora PostgreSQL, utilitzant AWS Schema Conversion Tool (SCT) i AWS Data Migration Service (DMS):

<https://docs.aws.amazon.com/prescriptive-guidance/latest/patterns/migrate-data-from-an-on-premises-oracle-database-to-aurora-postgresql.html>

L'adjudicatari haurà de dur a terme les següents tasques:

- Definició del pla de migració: conversió i migració de les dades.
- Suport a la execució del pla de migració per l'entorn de preproducció.
- Suport a la execució del pla de migració per l'entorn de producció.
- Validació de les dades migrades.

4.4 DevSecOps

S'entén per DevOps, el conjunt de pràctiques que pretenen aconseguir una sinèrgia en l'àmbit del desenvolupament de software (Dev) i l'àmbit d'operacions (Ops). DevSecOps incorpora pràctiques per fer que la seguretat sigui part del cicle de desenvolupament de software amb millors pràctiques de codificació segura i automatització de proves, entre d'altres.

Actualment PSIS disposa d'una infraestructura DevOps basada en Git, Jenkins i CloudFormation.

L'adjudicatari haurà de conèixer i utilitzar el model DevOps implantat per PSIS. En cas de que sigui necessari, l'adjudicatari haurà de ser capaç de:

- Mantenir els scripts de desplegament de CloudFormation.
- Integració Contínua (CI o *Continuous Integration*) / Lliurament Continu (CD o *Continuous Deployment*): Mantenir les pipelines Jenkins de construcció i pipelines de lliurament/desplegament per a les diferents unitats de desplegament i les seves versions.
- Infraestructura com a codi (IaC o *Infrastructure as Code*) & Gestió de Configuració Integrada (CM o *Configuration Management*): Mantenir les pipelines de construcció de la infraestructura en Cloud.
- Seguretat i Proves Integrades: Automatització de verificacions de seguretat com SAST (*Static Application Security Testing*), DAST (*Dynamic Application Security Testing*), i execució de proves de validació del funcionament de l'aplicació i les seves diferents parts.
- Tenir en compte que els desplegaments de canvis o noves versions s'han de poder fer en calent sense tall de servei.

4.5 Equip de projecte

Per garantir la màxima eficiència, desenvolupament, control i coordinació de les tasques d'aquest contracte, l'adjudicatari haurà de disposar d'un equip amb coneixement tecnològic de les aplicacions a desenvolupar.

A continuació, s'indiquen els perfils mínims exigits pel desenvolupament d'aquesta primera fase:

- 1 Cap de Projectes (dedicació 10%)
- 1 Arquitecte de Solucions AWS (dedicació 25%)

- 1 Enginyer de Software (dedicació 30%)
- 2 Desenvolupador Java/J2EE (dedicació 100%)
- 1 Enginyer Kubernetes i DevOps (dedicació 50%)

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

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. En aquests casos, es fixarà un temps de 2 setmanes de formació/adaptació del nou membre que anirà a càrrec de l'adjudicatari.

Caldrà acordar el calendari de canvi amb el Consorci AOC per tal de minimitzar l'impacte en els desenvolupaments en curs.

L'adjudicatari pot presentar perfils superiors als mínims exigits, però mai inferiors.

4.6 Coordinació amb la Oficina Tècnica de manteniment evolutiu i correctiu

La Oficina Tècnica de manteniment evolutiu i correctiu de PSIS realitza tasques de correcció de bugs i desenvolupament d'evolutius, sobre el mateix codi de PSIS 8.0. Serà l'encarregada de dur a terme els següents evolutius:

- Implementació dels nous estàndards de signatura electrònica del reglament europeu eIDAS (electronic IDentification, Authentication and trust Services).
- Refactorització del Truststore de PSIS basat en TSLs (Trust Service status List).
- Integració de PSIS amb una autoritat de segellat de temps reconeguda. Està previst substituir la TSA de PSIS per una TSA qualificada, és a dir, que compleixi amb els requeriments del reglament eIDAS. Caldrà integrar PSIS amb la TSA qualificada per dur a terme les funcions de completat de signatures.

Alguns d'aquests evolutius ja estaran en fase d'implementació o inclús finalitzats en el moment d'adjudicació del present contracte.

Caldrà que l'adjudicatari treballi conjuntament amb la oficina tècnica de manteniment evolutiu i correctiu per tal de coordinar els diferents evolutius que duran a terme en paral·lel ambdues oficines tècniques.

4.7 Requeriments funcionals

Aquest projecte es centrarà en les següents activitats:

- La execució del contracte s'iniciarà en la data de formalització del mateix.
- La gestió i el control del codi font es duran a terme amb el sistema centralitzat de codi font de que disposa el Consorci AOC (basat en el sistema de control de versions Git).
- L'adjudicatari serà el responsable de la definició del pla de proves d'integració i de rendiment, i de la seva execució als entorns de desenvolupament, preproducció i producció.
- L'adjudicatari per tant serà el responsable del control de qualitat i de validar el bon funcionament dels evolutius tant a nivell funcional com tècnic.
- L'adjudicatari haurà de preparar els paquets de desplegament pels entorns de desenvolupament, preproducció i producció.
- L'adjudicatari haurà d'elaborar la documentació tècnica i els manuals corresponents, així com mantenir actualitzada la documentació existent.

- L'adjudicatari haurà de prestar la formació que determini el Consorci AOC quan aquest ho consideri necessari.
- Per a cadascuna de les tasques anteriors, l'adjudicatari haurà de proporcionar els següents lliurables:
 - Anàlisi funcional.
 - Disseny tècnic.
 - Plans de proves unitàries i d'integració.
 - Manual d'explotació.
 - Codi font en el sistema centralitzat del Consorci AOC.
 - Desplegament a l'entorn de desenvolupament.
 - Procediment de desplegament als entorns de preproducció i producció del Consorci AOC.
- Aplicar controls de qualitat. L'adjudicatari serà el responsable del control de qualitat del servei en tots aquells desenvolupaments de nous evolutius que realitzi. En particular haurà de dur a terme les següents tasques:
 - Definició dels indicadors i mètriques de qualitat que han de complir els evolutius i identificar les mesures que s'utilitzaran per avaluar la qualitat.
 - Control de qualitat dels evolutius. Validació del funcionament correcte d'aquests tant a nivell funcional com tècnic, mitjançant l'execució de:
 - Proves unitàries.
 - Proves d'integració.
 - Proves funcionals.
 - Proves de regressió.
 - Proves de rendiment.
 - Suport als equips de desenvolupament mitjançant la definició dels estàndards i directrius que han de complir tots els evolutius per a ser certificats.
 - Revisió i auditoria del compliment d'aquests estàndards/directrius per assegurar que se segueixen els procediments establerts.
 - Revisió i seguiment de la qualitat de la documentació generada pels equips de desenvolupament.

4.8 Requeriments tècnics

4.8.1 Infraestructura necessària per dur a terme el desenvolupament del projecte

L'adjudicatari aportarà les infraestructures informàtiques, llicències de desenvolupament i qualsevol altre component o mitjà tècnic necessari per a la realització dels treballs.

L'entorn de desenvolupament basat en els serveis d'AWS serà proporcionat pel Consorci AOC.

L'adjudicatari mantindrà en tot moment l'actualització del codi font en el sistema de control de versions del Consorci AOC.

L'execució de les tasques encomanades s'haurà de poder dur a terme a les instal·lacions de l'adjudicatari, però és possible que en alguna ocasió sigui necessari el desplaçament d'algun dels membres de l'equip de l'adjudicatari a les instal·lacions del Consorci AOC.

4.8.2 Dimensionament

La nova solució ha d'estar dimensionada per poder absorbir sense degradació del servei els volums d'operacions prevists. Per tant, la infraestructura i l'arquitectura han d'estar dissenyades per poder escalar les necessitats puntuals d'un augment de peticions al servei.

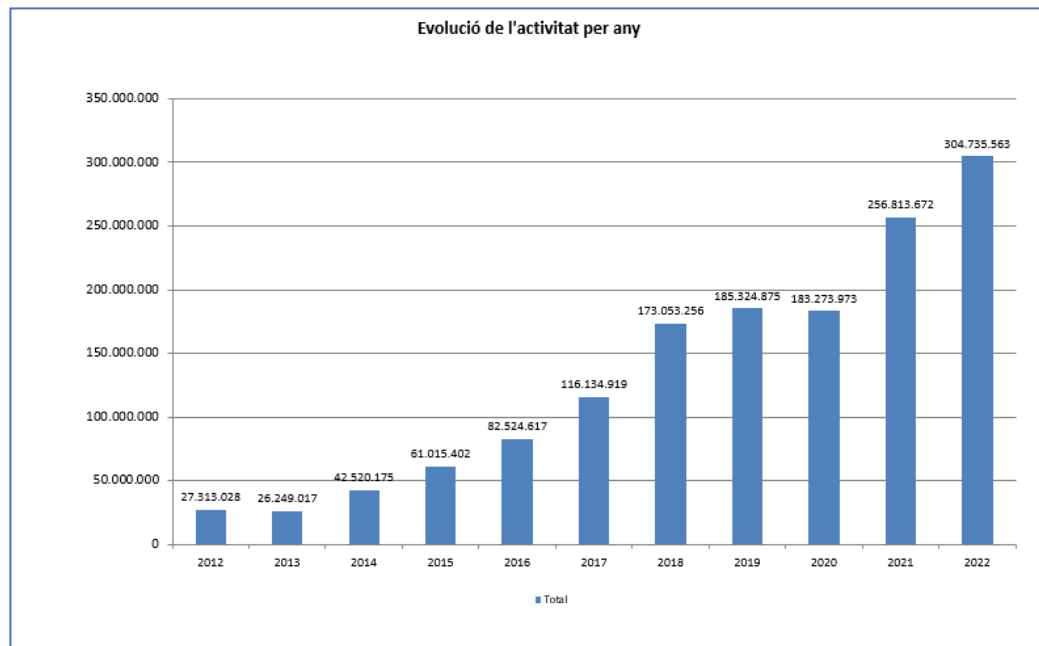
La nova arquitectura ha de donar resposta als següents requeriments tècnics:

- SLA

El servei de PSIS és **24x7**. No ens podem permetre aturades del servei en cap moment. És indispensable garantir el millor rendiment possible per continuar oferint un **SLA per sobre del 99.5%**.

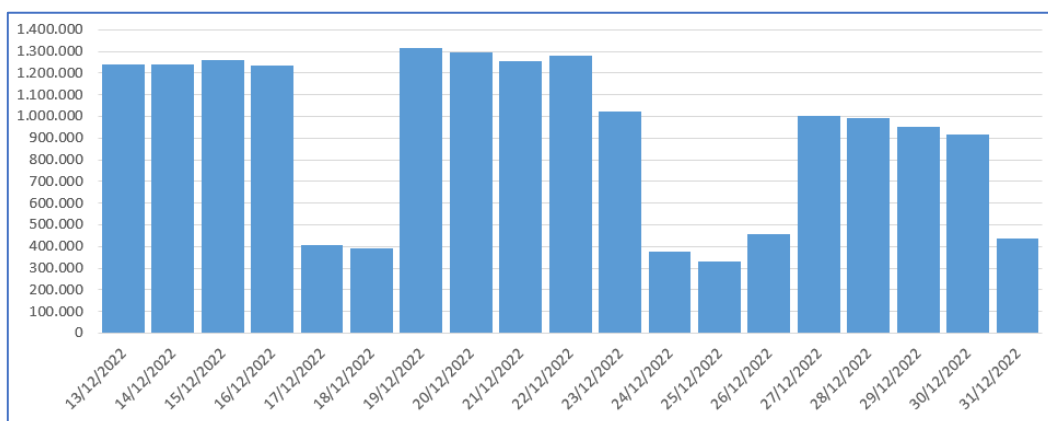
- Volumetries

PSIS és un servei transversal a la resta de serveis del Consorci AOC i en general de les AAPP catalanes. Té per tant un consum molt elevat, amb **més de 300 milions d'operacions anuals**. El volum d'operacions creix a mida que les administracions digitalitzen els seus processos, amb la qual cosa es preveu un increment important a mig/llarg termini. El creixement des de 2012 ha estat el següent:

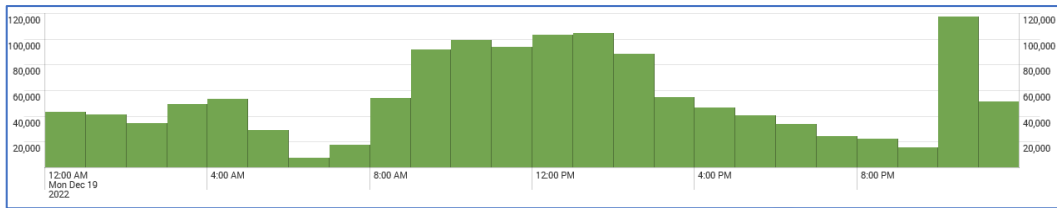


La volumetria actual en operacions de client és:

- El número total en 2022 va ser de més de 300 milions d'operacions.
- El volum mensual actualment és de l'ordre de **28 milions d'operacions mensuals de mitjana**. Aquest número oscil·la entre 20 i més de 32 milions d'operacions mensuals.
- El **volum de peticions diàries** pot oscil·lar entre **300.000 i 1,3 milions**. Per exemple, al següent gràfic tenim el volum de peticions diàries durant les dues últimes setmanes del mes de desembre de 2022:



El tràfic de peticions en PSIS és continu. Tanmateix aquest tràfic no es distribueix de manera uniforme durant el dia, sinó que en certes franges el volum de peticions és més concentrat. Per exemple:



La solució ha de poder absorbir, a l'entorn productiu, sense degradació dels temps de resposta, com a mínim:

- **3.000 operacions de client per minut.**
- **50 operacions concurrents** amb temps migs de resposta inferiors a 1 segon.
- Temps de resposta

Els temps de resposta de PSIS han de ser de **mil·lisegons**. Només les operacions de validació i completat de signatures o documents poden tenir puntualment temps de resposta de l'ordre de pocs segons depenent de l'antiguitat i la complexitat de la signatura.

Òbviament els temps de resposta de PSIS es poden veure compromesos per la forta dependència d'aquests vers els serveis de revocació de tercers.

El temps mig de resposta pels diferents tipus d'operacions han de ser de l'ordre de:

- Validació de certificats: **inferior a 100 mseg**
- Validació i completat de signatures i documents signats: **inferior a 300 mseg**
- Creació de segells de temps: **inferior a 100 mseg**
- Creació de signatura: **inferiors a 2 segons** (cal dir que aquest valor correspon a les signatures d'iArxiu, que són especialment complexes).
- Guardat d'evidències legals: **inferior a 50 mseg**

El Consorci AOC valorarà molt positivament qualsevol reducció dels temps de resposta.

4.8.3 Codi font i propietat intel·lectual

La gestió i control del codi font es durà a terme amb el sistema centralitzat de codi font de que disposa el Consorci AOC (basat en el sistema de control de versions Git).

L'adjudicatari accepta expressament que la propietat de tots els lliurables, independentment de la seva naturalesa, així com dels resultats dels treballs realitzats, i en particular els productes i serveis objecte del contracte, correspon únicament al Consorci AOC amb exclusivitat i amb caràcter general, sense que l'adjudicatari pugui conservar, ni obtenir còpia dels mateixos o facilitar-lo a tercers.

L'adjudicatari no podrà fer cap ús o divulgació dels estudis i documents utilitzats o elaborats com a resultat de la prestació del servei objecte del contracte, bé sigui en forma total o parcial, original o reproduïda, sense autorització expressa del Consorci AOC, que la donaria, si escau, prèvia petició formal de l'adjudicatari amb indicació expressa de la finalitat.

4.8.4 Tests unitaris i proves d'integració

L'adjudicatari haurà d'implementar un joc exhaustiu de proves unitàries i d'integració per validar tots i cadascun dels serveis implementats al llarg del desenvolupament de PSIS 9.0.

L'adjudicatari haurà d'executar aquests jocs de proves als entorns de desenvolupament, preproducció i producció del Consorci AOC una vegada s'hagi executat la posada en marxa i

explotació i s'hagi realitzat el desplegament de la nova solució als entorns AWS del Consorci AOC.

4.8.5 Tests de rendiment

Durant el desenvolupament i al final del projecte, l'adjudicatari haurà de proporcionar jocs de proves de càrrega i test d'estrès per validar que PSIS 9.0 compleix amb els requeriments tècnics i funcionals.

4.9 Requeriments legals

PSIS 9.0 ha de ser un servei qualificable, és a dir:

- La solució proposada haurà de complir amb els requisits que estableix la norma **ETSI EN 319.401** "General Policy Requirements for Trust Service Providers", en relació a la gestió i operació del servei.
- La solució haurà de complir amb l'especificació tècnica **ETSI TS 119.441** "Policy requirements for TSP providing signature validation services", la qual estableix requisits específics de gestió i operació d'un servei específic de validació.
- PSIS està catalogat com a servei de **nivell alt** segons l'**Esquema Nacional de Seguretat** (ENS). La valoració de PSIS per a cada dimensió de seguretat és la que s'exposa a la taula següent. La solució haurà d'aplicar tots els controls que apareixen en l'annex II de l'ENS d'acord amb la valoració de cada dimensió de seguretat.

	RGDP	ENS					
SERVEI	Dades Personals	Confidencialitat	Disponibilitat	Autenticitat	Integritat	Traçabilitat	RTO
Definicions	Les conseqüències que tindria sobre les persones la revelació a persones no autoritzades o que no necessiten conèixer la informació.	Les conseqüències que tindria la seva revelació a persones no autoritzades o que no necessiten conèixer la informació.	Les conseqüències que tindria el no poder comprovar a posteriori qui ha accedit a, o modificat, una certa informació.	Les conseqüències que tindria el fet que la informació no fos autèntica.	Les conseqüències que tindria la seva modificació per algú que no està autoritzat a modificar la informació.	Les conseqüències que tindria el no poder comprovar a posteriori qui ha accedit a, o modificat, una certa informació.	Temps màxim de recuperació del servei en cas d'Indisponibilitat.
Validador PSIS	Mitja	Mitja	Alta	Alta	Mitja	Alta	<4h

RGDP: Reglament General de Protecció de Dades

ENS: Esquema Nacional de Seguretat

RTO: Objectiu de Temps de Recuperació

4.10 Requeriments de seguretat

4.10.1 Mesures de seguretat que ha d'incorporar PSIS 9.0 com a solució

Durant el temps d'execució del contracte, l'adjudicatari haurà d'implementar les mesures de seguretat de nivell alt de l'Esquema Nacional de Seguretat que afecten directament a PSIS 9.0 com a solució i plataforma tecnològica. Concretament són les descrites a:

- Annex4_Taula aplicabilitat_ENS_P SIS.xlsx** (per descarregar aneu al punt 5 Annexos)

4.10.2 Mesures de seguretat a complir per part de l'adjudicatari

4.10.2.1 Certificacions de seguretat

Durant el temps d'execució del contracte, l'adjudicatari haurà d'implementar les mesures de seguretat de nivell mig de l'Esquema Nacional de Seguretat. Concretament són les descrites a:

- ***Annex5_Requeriment_de_seguretat_(ENS)_pels_proveïdors_de_software.pdf*** i que són les que afecten a l'adjudicatari com a part del sistema PSIS 9.0. (per descarregar aneu al punt 5 Annexos)

El Consorci AOC auditarà en un termini no superior a 6 mesos, que l'adjudicatari compleix amb els requeriments que es detallen al document annex *Annex5_Requeriment_de_seguretat_(ENS)_pels_proveïdors_de_software.pdf*. L'auditoria es farà mitjançant la entrega de les evidències indicades en l'annex al Consorci AOC per a que aquest determini el grau de compliment.

L'adjudicatari estarà exempt de l'auditoria si aporta una certificació vigent de l'Esquema Nacional de Seguretat de nivell baix expedit per una empresa certificadora independent i homologada.

En cas d'auditoria externa de PSIS, l'adjudicatari haurà de participar en l'auditoria en les tasques que li corresponguin, entregant les evidències que l'auditor reclami i fent les adequacions necessàries que els hi pertoquin.

4.10.2.2 Control d'accés al sistema

L'adjudicatari haurà de adaptar-se en tot moment als mecanismes de control d'accés als sistemes d'informació que imposi el Consorci AOC per accedir als seus sistemes.

4.10.2.3 Control de personal

L'adjudicatari haurà d'informar en tot moment de les altes i baixes del personal intern o subcontractat que en nom seu accedeixi als sistemes del Consorci AOC.

En cas de baixa d'un usuari, de manera immediata l'adjudicatari haurà d'informar al Consorci AOC per tal de revocar els seus drets d'accés als sistemes.

4.10.2.4 Protecció de la informació

L'adjudicatari no podrà fer ús de les dades reals dels sistemes de producció en els sistemes de desenvolupament.

L'adjudicatari no podrà descarregar informació del Consorci AOC en els seus sistemes o en suports portàtils com USBs, DVDs, portàtils, tablettes, etc. En el cas d'haver de fer-ho caldrà demanar l'autorització del Consorci AOC i el suport haurà d'estar xifrat.

Els fitxers temporals que s'haguessin creat exclusivament per la realització de treballs temporals auxiliars hauran de complir amb les mesures establertes que s'apliquin als fitxers considerats definitius.

Tot fitxer temporal així creat serà esborrat una vegada hagi deixat de ser necessari per la finalitat que va motivar la seva creació.

Al finalitzar la relació laboral entre el Consorci AOC i l'adjudicatari, aquest haurà d'entregar tota la informació propietat del Consorci AOC (procediments, codi font, etc.) i fer un esborrat segur dels suports on aquesta estigui emmagatzemada.

El contracte ha de determinar la propietat de la informació a la que tindrà accés l'adjudicatari, ja sigui de la part contractant o de terceres parts.

L'adjudicatari ha de comprometre's en el contracte a mantenir la confidencialitat en el tractament de la informació del client, comprometre's per contracte a no divulgar o accedir indegudament a

la informació sense l'autorització expressa del seu propietari. L'adjudicatari queda obligat a no accedir ni utilitzar la informació a la qual tingui accés per a qualsevol fi que no estigui explicat en el contracte o s'autoritzi expressament per escrit amb posterioritat a la signatura del contracte.

4.10.2.5 Protecció dels suports

L'adjudicatari no pot descarregar informació del Consorci AOC en els seus sistemes. En cas d'haver de fer-ho caldrà demanar l'autorització del Consorci AOC, i si aquesta és concedida els suports es protegiran de la següent manera:

- Els suports d'informació amb dades del Consorci AOC s'han d'identificar mitjançant etiquetatge o mecanisme equivalent de forma que, sense revelar el seu contingut, s'indiqui el nivell de seguretat de la informació continguda de més qualificació.
- Les etiquetes o mecanismes equivalents haurien de ser fàcilment identificables. S'informarà als usuaris sobre aquests mecanismes d'identificació per tal que, o bé mitjançant simple inspecció, o bé mitjançant el recurs a un repositori, puguin entendre el significat.
- Es podrà excloure, per previsió a la normativa, l'obligació d'etiquetatge en cas de suports en que no es pugués complir per les seves característiques físiques, establint mesures alternatives per assegurar la seva identificació i localització.
- Els suports d'informació que s'hagin de reutilitzar per a una altra informació o lliurar a una altra organització han de ser objecte d'un esborrat segur del seu contingut.

S'han de destruir de manera segura els suports d'informació, en els casos següents:

- Quan la naturalesa del suport no permeti un esborrat segur.
- Quan així ho requereixi el procediment associat al tipus d'informació continguda.

S'han d'aplicar mecanismes de xifrat que garanteixin la confidencialitat i la integritat de la informació continguda en tots els suports.

4.11 Requeriments de protecció de dades

Per cada àmbit objecte d'anàlisi que comporti el tractament de dades de caràcter personal caldrà fer un informe de les mesures a adoptar per implantar les mesures de privacitat des del disseny i per defecte 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. L'informe haurà de contenir l'anàlisi de quins principis del Reglament permet donar compliment cadascuna de les mesures aportades, justificant-ho també en base a la normativa específica que regula l'àmbit d'actuació de les administracions usuàries del servei i l'adequació de cada mesura proposada en relació al seu propòsit de complir els principis de protecció de dades i reduir el risc pels drets i les llibertats.

Caldrà tenir en compte com a mínim les Guies publicades tant pel Comitè Europeu de Protecció de Dades com per l'Agència Espanyola de Protecció de Dades i les que pugui publicar l'Autoritat Catalana de Protecció de dades.

4.12 Pla de devolució del servei

Al final del servei l'adjudicatari haurà de planificar i executar el pla de devolució del servei al Consorci AOC.

Aquest pla constarà com a mínim del manual detallat d'instal·lació i posada en marxa, i dels paquets de desplegament pels entorns de desenvolupament, preproducció i producció. En el cas

de que al llarg del projecte PSIS 9.0 no estigui desplegat als entorns de preproducció i producció, l'adjudicatari haurà de donar posteriorment suport a la posada en marxa en aquests entorns.

L'adjudicatari lliurarà al Consorci AOC les fonts dels programes informàtics, els manuals, estudis, informes, anàlisis i d'altres productes, en bon estat de conservació i funcionament.

4.13 Condicions d'execució

4.13.1 Obligacions bàsiques

L'adjudicatari haurà de complir les següents obligacions bàsiques:

- El Consorci AOC es farà càrrec de les dues primeres setmanes de formació en l'aplicació PSIS. Tot el temps que excedeixi d'aquestes dues setmanes i fins que es comencin els treballs, serà a càrrec de l'empresa licitadora.
- Gestionar qualsevol alteració del servei en les condicions expressades en aquest plec.
- L'adjudicatari haurà de calcular l'esforç necessari per dur a terme cadascun dels evolutius pactats. Periòdicament l'adjudicatari farà arribar al Consorci AOC les hores dedicades a cadascun dels evolutius en curs. S'establiran controls entre el volum d'hores executades i els objectius assolits. En cas de que algun desenvolupament es desviï en gran mesura de les previsions inicials i aquest desviament no es correspongui a un canvi de requeriments per part del Consorci AOC ni sigui tècnicament justificable, l'adjudicatari haurà d'assumir part dels costos extra, sempre que el Consorci AOC així ho consideri.
- Realitzar reunions periòdiques amb el Consorci AOC per tal d'exposar el compliment del servei i tractar els possibles problemes o millores del servei.
- Realitzar la formació dels tècnics designats, en tots aquells aspectes que el Consorci AOC cregui oportuns i que siguin de directa aplicació als serveis requerits.
- Tota la documentació generada per l'equip serà en català i en el format proposat per Consorci AOC.
- Presentació d'informes mensuals de presentació del servei d'acord amb els indicadors que el Consorci AOC consideri apropiats:
 - Informe resum de les actuacions ja resoltes (micro-projectes) i hores realitzades.
 - Informe de situació de les actuacions en curs i hores realitzades.
 - Informe resum de les actuacions pendents i hores estimades.
 - Planificació de les actuacions a realitzar.
 - Escandall del total d'hores realitzades durant el mes.
- Definir una forma de treball basada en metodologies del tipus Agile o basada en micro-projectes.

4.13.2 Eines de control

Les eines de control corporatives del Consorci AOC són, principalment, Jira i Microsoft Teams. I són les que es faran servir per dur a terme la gestió del projecte.

L'adjudicatari serà responsable de:

- Proposar les eines addicionals a les eines corporatives del Consorci AOC, que han de permetre el seguiment i el control global del contracte.
- El Consorci AOC es reserva el dret a validar, i si s'escau a definir, les eines que s'hagin de fer servir per la gestió i el control del servei.

4.13.3 Normativa aplicable

L'adjudicatari es compromet a complir els requeriments de seguretat, qualitat i continuïtat aplicables a l'objecte del contracte especificats a:

- La legislació vigent en general i, en particular, quan es tractin dades de caràcter personal, el Reglament UE 2106/679 del Parlament europeu i del Consell, de 27 d'abril de 2016 relatiu a la protecció de les persones físiques pel que respecta al tractament de dades personals. A més de l'establert en el Plec de clàusules administratives particulars, per cada mòdul funcional que impliqui el tractament de dades de caràcter personal caldrà aportar un informe justificatiu de l'anàlisi de l'impacte del mateix sobre les dades afectades i la justificació de les mesures implantades per donar compliment a la normativa vigent.
- ISO/IEC 27001 de seguretat de la informació o l'Esquema Nacional de Seguretat.

4.14 Model de relació

L'adjudicatari haurà d'explicar en la seva proposta quin és el model de relació que proposa per garantir l'èxit del projecte.

Com a mínim, però, caldrà establir els següents nivells d'interlocució:

- Reunions d'estratègia i direcció amb les següents característiques:
 - Interlocutors: Responsable del servei per part de l'adjudicatari, Cap de Servei per part del Consorci AOC.
 - Periodicitat: Mensual
 - Objectiu: Fer el seguiment del contracte, analitzant diversos aspectes: productivitat, control d'hores, temes de facturació, seguiment de fites (a alt nivell), etc.
 - Lliurables: Actes de les reunions, informes executius, informes amb control d'hores (fetes i pendents), etc.
- Reunions de seguiment amb les següents característiques:
 - Interlocutors: Les persones assignades per l'adjudicatari per dur a terme el servei. Per part del Consorci AOC serà el Cap de Projectes o algun dels tècnics assignats al projecte.
 - Periodicitat: Setmanal
 - Objectiu: Seguiment detallat de les fites i del pla de projecte i gestió de les incidències o desviaments més destacables.
 - Lliurables:
 - Informe resum de les actuacions ja resoltes i hores realitzades.
 - Informe de situació de les actuacions en curs i hores realitzades.
 - Informe resum de les actuacions pendents i hores estimades.
 - Planificació de les actuacions a realitzar.
 - Escandall d'hores totals realitzades durant el mes el curs.
- Reunions de coordinació amb la oficina tècnica actual de manteniment evolutiu i correctiu de PSIS:
 - Interlocutors: Les persones assignades per l'adjudicatari. Per part de la Oficina Tècnica actual serà el Cap de Projectes o algun dels tècnics assignats al projecte.
 - Periodicitat: Setmanal com a mínim; a determinar en funció de les necessitats.
 - Objectiu: Coordinació d'ambdues oficines tècniques en relació als evolutius que s'estiguin duent a terme en paral·lel per cadascuna d'elles.
- Reunions de treball per anar avançant i concretant els aspectes del projecte mitjançant una metodologia del tipus àgil.

5 Annexos

En aquest apartat trobareu documents de referència que expliquen com és l'actual PSIS 6.0, així com la definició de l'arquitectura de PSIS 8.0.

Tots aquests annexos els podeu consultar en el següent enllaç:

<https://licenciasaoc.sharepoint.com/:f:/s/Tecnologia/Ejl50ow4XrxJgGwgqK92AjwtBDGIkjNJt1RpDkntYZq7Hbw?e=n3ydo7>

- Annex 1 - Descripció tecnològica de PSIS 6.0
- Annex 2 - Arquitectura de PSIS 6.0
- Annex 3 - Definició de l'arquitectura de PSIS 8.0
- Annex 4 - Taula aplicabilitat ENS PSIS
- Annex 5 - Requeriment de seguretat (ENS) pels proveïdors de software

Barcelona

Áurea Alcaide Izquierdo

Àrea de Tecnologia del Consorci AOC