PLEC DE PRESCRIPCIONS TÈCNIQUES DEL CONTRACTE DE SERVEI D'APLICACIÓ MÒBIL IDCAT

Realitzat per: Consorci AOC

Versió: 1.0

Data: 26/6/2024

Arxiu: 2023 Contracte servei Aplicació Mòbil idCAT NGEU - Plec Tècnic

Índex

1 Introducció ... 3
2 Context ... 4
2.1 Situació actual ... 4
2.1.1 Identitat digital ... 4
2.1.2 Catalunya com país líder en Identitat Digital ... 4
2.1.3 Problemàtiques actuals ... 5
2.1.4 Videoidentificació ... 6
2.1.5 Signatura remota ... 6
2.1.6 Identitat autogestionada ... 6
2.1.7 Marc europeu ... 6
2.2 Serveis d'identificació i signatura electrònica per a la ciutadania del Consorci AOC ... 7
2.2.1 Credencials per a la ciutadania ... 7
2.3 Bus d'integració de mecanismes d'identificació i signatura electrònica ... 8
2.4 Signador ... 8
3 Calendari, fites i objectius ... 9
4 Objecte del contracte ... 10
5 Activitats i funcions de l'empresa contractista ... 11
6 Requisits generals obligatoris ... 12
6.1 Requisits generals obligatoris ... 12
6.1.1 Normativa vigent de compliment obligat ... 12
6.1.2 Requisits funcionals ... 12
6.1.3 Requisits de protecció de dades ... 13
6.2 Funcionalitats mínimes a desenvolupar ... 14
6.3 Serveis tecnològics ... 15
7 Formes de seguiment i control de l'execució de les condicions ... 16
8 Aspectes de seguretat i ENS ... 17

1 Introducció

El contingut d'aquestes prescripcions tècniques deriva del projecte "Plataforma comuna de gestió i analítica de dades per les administracions catalanes" amb codi C11.I03.P04.S14, aprovat en el marc del Mecanisme de Recuperació i Resiliència (MRR), regulat pel reglament 2021/241 del Parlament Europeu i del Consell de 12 de febrer de 2021.

Amb la mera presentació de la seva oferta, l'empresa licitadora accepta les prescripcions tècniques establertes en aquest plec.

Qualsevol proposta que no s'ajusti als requeriments mínims establerts en aquest plec quedarà automàticament exclosa de la licitació.

2 Context

2.1 Situació actual

2.1.1 Identitat digital

La identitat digital ha emergit amb força els darrers anys, degut al desenvolupament de l'economia digital, dels serveis de l'administració electrònica i de la seva utilització de forma quotidiana per la gran majoria de la ciutadania. Actualment, més del 80% dels ciutadans de Catalunya són internautes habituals que accedeixen periòdicament a Internet i a serveis en línia. I la majoria d'interaccions entre els ciutadans, les empreses i les Administracions requereixen de disposar d'una identitat digital. Els governs i els negocis enfronten la necessitat d'identificar a les persones amb suficients garanties, de forma fiable i correcta, per a realitzar les transaccions de processos de negoci amb seguretat.

La identitat digital s'ha convertit en un element tractor clau de la transformació digital, com ho demostren els països del món més avançats en la societat de la informació. Al mateix temps, en els territoris on les solucions d'identitat digital desenvolupades no compleixen els criteris de ser fàcils, segures i de confiança, s'ha convertit en una barrera del desenvolupament digital.

Catalunya ha estat un país líder en identitat digital, per bé que especialment en la vessant aplicada a l'Administració electrònica.

2.1.2 Catalunya com país líder en Identitat Digital

En desenvolupament del pacte institucional signat el 23 de juliol del 2001 pels grups parlamentaris del Parlament de Catalunya, la Generalitat de Catalunya i el Consorci d'Ens Locals de Catalunya (Localret), es va decidir establir sistemes d'interrelació entre les esmentades administracions, i entre les administracions i els ciutadans, per via telemàtica i electrònica, en les condicions de seguretat necessàries i, especialment, fent ús de certificats digitals d'identitat i signatura electrònica.

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

D'aquesta forma, CATCert es va constituir en l'entitat principal del sistema públic català de certificació que regula l'emissió i la gestió dels certificats que s'emetin per a les entitats que integren el sector públic català; així com l'admissió i l'ús dels certificats emesos a ciutadans i empreses per a altres prestadors de serveis de certificació qualificats.

D'acord a la Llei 29/2010, del 3 d'agost, de l'ús dels mitjans electrònics al sector públic de Catalunya, CATCert té la competència de prestar serveis de signatura electrònica al sector públic de Catalunya per a garantir la confidencialitat, la integritat, la identitat i el no-rebuig en les comunicacions electròniques que duen a terme les entitats del sector públic de Catalunya, i qualsevol altra tasca que se li encomani. Posteriorment aquestes funcions van ser assumides pel Consorci AOC directament, en virtut de l'absorció del CATCert.

El Consorci AOC genera, actualment, dos tipus de certificats: l'idCAT certificat, per a la ciutadania i sense cost; i la T-CAT, per als càrrecs electes i empleats públics. Al 2015 es va desenvolupar la solució idCAT Mòbil, que utilitza un sistema de doble factor d'autenticació basat en codis d'un sol ús enviats per SMS. Els sistemes d'identificació basats en dispositiu en mòbil són més usables, més fàcils d'obtenir i més econòmics. Tot plegat fa que el seu grau d'implantació, ús i satisfacció per a la ciutadania sigui molt més alt que el dels certificats digitals.

El Consorci AOC disposa d'una xarxa d'entitats de registre per a facilitar als ciutadans identitats digitals pel canal presencial. Aquesta xarxa té actualment prop de 400 oficines d'entitat de

registre de 280 ens diferents desplegades a tot el territori de Catalunya, garantint que els ciutadans tenen a una distància raonable (al seu Ajuntament, capital de comarca o oficina de la Generalitat) un punt on obtenir de forma immediata una identitat digital basada en certificat (idCAT certificat) o basada en doble factor mitjançant un dispositiu mòbil (idCAT Mòbil).

Per la seva banda, l'Administració General de l'Estat ofereix el servei Cl@ve, que utilitza un sistema de doble factor basat en codis d'un sol ús enviats per SMS i possibilita la signatura electrònica "al núvol".

2.1.3 Problemàtiques actuals

Resulta evident que els desenvolupaments tècnics i legals esmentats, els canvis socials en l'adopció de noves tecnologies i les noves demandes de la ciutadania han generat una necessitat de canvi urgent per tal de mantenir aquest lideratge. Concretament cal donar resposta a les següents mancances i problemàtiques actuals:

- **La obsolescència de les polítiques públiques d'identitat digital**, que tradicionalment han prioritzat la identitat basada en el certificat digital. El certificat digital ha demostrat ser una eina útil al llarg de tots aquests anys per als usuaris que tenen una relació intensiva amb l'administració pública: empreses, gestors, col·legiats, entitats, etc. Ara bé, el seu ús és molt baix per als ciutadans que tenen una relació esporàdica amb l'administració (que són la gran majoria) atesa la seva relativament baixa usabilitat i a la dificultat en la resolució de incidències sense suport tècnic especialitzat. El certificat digital continuarà sent un instrument important per a determinats col·lectius, però cal modernitzar-lo, adequar-lo a la mobilitat i ampliar-ne les funcionalitats, per garantir que resulti un instrument útil i atractiu per als seus usuaris.
- **La fragmentació de la identitat digital**, en la mesura que han aparegut nombrosos prestadors, tant públics com especialment privats, que ofereixin serveis d'identitat digital als ciutadans, que poden tenir dificultats per entendre el valor de cada mecanisme. Actualment, un usuari internauta actiu té, de mitjana, més de cinquanta credencials per accedir a diferents serveis d'internet. Aquesta fragmentació fa que la seva gestió sigui molt ineficient, generi importants costos personals i a les organitzacions, i suposi un greu problema de seguretat per manca de manteniment adequat d'aquestes credencials, per la seva repetició o per simplement escriure aquestes credencials en espais que poden ser accessibles per tercers.
- **La desorientació del ciutadà** entre les diferents identitats que li va creant cada administració o prestador de serveis per relacionar-se millor amb ells, i les dificultats d'ús entre elles. Les enquestes de satisfacció que realitza periòdicament el Consorci AOC demostren que els sistemes d'identificació digital de doble factor d'autenticació basats en dispositius mòbils tenen un grau de satisfacció molt més alt que els certificats digitals, atesa la seva usabilitat i facilitat de registre.
- **El baix ús dels serveis públics electrònics**, degut a la insuficient acceptació i utilització dels mecanismes d'identitat digital actuals.
- **La menor capacitat per prestar serveis innovadors** en l'àmbit de la societat de la informació i de l'administració electrònica, per la fragmentació de la identitat digital.
- **La ciutadania ha perdut el control de les seves dades personals i s'ha creat una monopolització per part de les grans plataformes digitals** que està creant situacions d'abús en la seva explotació. Aquest monopoli està generant una malfiança creixent en la ciutadania i les institucions públiques, que no afavoreix la creació d'una economia digital de confiança. A més, aquests abusos poden tenir un impacte en la privadesa i l'autonomia, i pot afectar a la seguretat de la identitat en línia de les persones. L'enorme quantitat de dades que es generen cada dia ofereixen moltes oportunitats per a millorar els serveis públics en línia i l'economia digital, però cal un model de governança que garanteixi clarament els drets digitals i la privacitat de la ciutadania, i alhora distribueixi de forma equitativa els beneficis de l'explotació d'aquestes dades.

2.1.4 Videoidentificació

Durant l'any 2020, especialment amb motiu de la crisi sanitària produïda per la pandèmia del COVID-19, es va posar de manifest la necessitat d'habilitar mètodes de registre per l'obtenció de credencials electròniques que no requereixi de la presencialitat física de la persona interessada. En el cas dels certificats electrònics qualificats, el Reglament Europeu 910/2014 d'identificació i serveis de confiança (en endavant ReIdAS) obre la porta, al seu article 24, a acceptar d'altres mecanismes amb un nivell de seguretat equivalent d'acord amb el dret nacional. A nivell estatal l'article 7 de la Llei 6/2020 reguladora de determinats aspectes dels serveis electrònics de confiança permet l'obtenció de certificats qualificats mitjançant vídeo identificació, sempre que aquest procés s'ajusti les condicions i requisits tècnics establerts per l'Ordre ETD/465/2021 del Ministeri d'Assumptes Econòmics i Transformació Digital.

Aquesta Llei genera una gran oportunitat per plantejar una solució que compleixi tots els requisits que demanda la ciutadania. L'objectiu del projecte és desenvolupar, provar i desplegar una aplicació mòbil (APP) per gestionar una identitat digital basada en certificats digital qualificats, que permeti la seva obtenció per Internet amb totes les garanties i que faciliti el seu ús en els processos d'autenticació i signatura electrònica mitjançant dispositius mòbils. També es podria plantejar la generació d'un "carnet" digital d'identificació electrònica en actuacions presencials.

Aprofitant aquesta nova possibilitat, tots els Prestadors de Serveis de Certificació treballen actualment per permetre el registre per videoidentificació. En aquesta línia, l'AOC ha implantat un procediment de registre per videoidentificació per idCAT Mòbil i treballa per poder oferir aquesta possibilitat també per als certificats idCAT.

2.1.5 Signatura remota

L'ús de certificats digitals, sobre tot pel ús en la signatura de documents, ha presentat i presenta problemes d'usabilitat que han dificultat la seva implantació. L'ús de les claus de signatura, especialment si aquestes estan hostatjades en un dispositiu criptogràfic, requereix que les aplicacions que les empren estiguin dissenyades especialment per fer-ho. En el cas dels navegadors web, que generalment no permeten aquest ús en processos de signatura de forma nativa i que ja no permet implementar-ho de forma externa, les persones que signen documents han de recorre a aplicacions externes.

Una possibilitat per mitigar aquests problemes consisteix en delegar els processos de gestió i custòdia de claus en serveis centralitzats, encarregats d'identificar a les seves persones usuàries i L'Annex II del ReIdAS permet als prestadors qualificats de serveis de confiança gestionar les claus de signatura en nom de la persones signatàries.

2.1.6 Identitat autogestionada

Precisament amb l'objectiu de tornar el control de les seves dades personals als usuaris, alguns organismes internacionals com W3C i la Decentralized Identity Foundation (DIF), comptant amb el suport dels actors més rellevants del sector, estan impulsant iniciatives per la descentralització de la identitat. Basant-se en l'emergent tecnologies de les Xarxes de Registre Distribuït i cadenes de blocs estan treballant en la creació d'un model d'identitat auto gestionada (Self-Sovereign identity - SSI), on el tercer de confiança deixa de tenir un paper clau en la gestió de les dades de caràcter personal, que passen a ser custodiades precisament pels propis usuaris.

Destacar en aquest sentit els treballs de W3C en la definició d'un marc conceptual[1], amb el seu format de document d'identitat estàndard, així com de declaracions verificades[2] que estan sent implementades per diferents solucions concretes sobre diferents xarxes de registre distribuït, tant públiques com privades, permissionades i no permissionades.

2.1.7 Marc europeu

Cal esmentar que el ReIdAS, separa clarament la identificació electrònica dels serveis de confiança, configurant la identitat digital com a servei públic, i els serveis de confiança com a mercantils, fins i tot quan són prestats per l'administració.

A més, al desenvolupament normatiu està prescrivint un escenari on el ciutadà és propietari de les seves identitats digitals i de les seves dades personals, tal i com preveu el nou Reglament General de Protecció de Dades (GDPR). Aquest apoderament de la ciutadania deriva en una major participació, conscienciació i accés, que també fonamenta els principis de la Llei 19/2013, del Govern espanyol, de Transparència, Accés a la informació pública i bon govern.

Al juny del 2021 es va presentar una proposta de modificació del ReIdAS que incorpora el concepte de cartera electrònica per la ciutadania amb funcionalitats de identificació, signatura electrònica i gestió d'atributs, amb l'objectiu de potenciar aquest empoderament.

2.2 Serveis d'identificació i signatura electrònica per a la ciutadania del Consorci AOC

2.2.1 Credencials per a la ciutadania

El Consorci AOC és el prestador de mecanismes d'identificació i serveis de confiança de les Administracions Públiques Catalanes. Com a tal, des del Consorci AOC s'emeten dues credencials per tal que els ciutadans es puguin relacionar telemàticament amb les administracions, garantint el compliment de la normativa tècnica i jurídica vigent.

- **idCAT Certificat.** És un certificat qualificat de signatura avançada d'acord amb el ReIdAS. És per tant un certificat en programari que els ciutadans poden obtenir adreçant-se, presencialment, a qualsevol dels ens que s'han establert com a entitat de registre del servei.
- **idCAT Mòbil.** És un mecanisme d'autenticació de dos factors basat en l'enviament de paraules de pas d'un sol ús per SMS al dispositiu mòbil del ciutadà. Per ser-ne usuari, cal que el ciutadà s'enregistri a la Base de Dades de la Seu Electrònica de la Generalitat de Catalunya. Aquest registre es pot portar a terme:
    - Presencialment, tant des de les entitats de registre del Consorci AOC com des de les OAC de la Generalitat de Catalunya.
    - Telemàticament:
        - emprant un certificat qualificat,
        - per videoidentificació, o
        - introduint dues dades conegudes i que el Consorci AOC pot verificar, com són la data de caducitat del DNI i el número TIS de targeta sanitària.

D'aquesta manera, el Consorci AOC, a través de la xarxa d'entitats de registre ja esmentada, ofereix la possibilitat d'obtenir, de forma immediata, una identitat digital basada en certificat (idCAT certificat) o basada en doble factor mitjançant un dispositiu mòbil (idCAT Mòbil).

El Consorci AOC també ofereix un servei, anomenat Via Oberta, que permet consultar de forma telemàtica les dades i documents electrònics procedents d'altres Administracions públiques i institucions (prestadors de dades), fent efectiu el dret dels interessats en el procediment administratiu a no aportar certificats i documentació en suport paper. És un servei pensat per a demostrar, de manera telemàtica, les atribucions de l'interessat en un procediment administratiu sense necessitat de que aquest aporti documentació addicional de forma presencial.

2.3 Bus d'integració de mecanismes d'identificació i signatura electrònica

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

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

2.4 Signador

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

3 Calendari, fites i objectius

El calendari per assolir les fites i objectius s'ajustarà al termini d'execució establert a partir de la data de formalització del contracte.

L'estimació dels terminis de cada fita, així com el seu abast, es determinarà en funció de la durada de cada període del contracte, distribuint-se de la següent manera:

1. Disseny del servei. Duració: 20% del termini d'execució
2. Prova de concepte funcional. Duració: 20% del termini d'execució
3. Pilotatge amb els usuaris. Duració: 20% del termini d'execució
4. Integracions i implantació del servei. Duració: 40% del termini d'execució

4 Objecte del contracte

L'objecte del contracte de la present licitació és un servei de l'aplicació mòbil idCAT que incorpora un mecanisme d'autenticació i signatura electrònica, la gestió i ús de les credencials d'identitat i l'accés al serveis digitals de l'AOC.

L'esquema de la Figura 1 mostra la relació que haurà de tenir l'aplicació mòbil amb la resta de serveis que el Consorci AOC ofereix relacionats amb la identificació i la signatura electrònica.

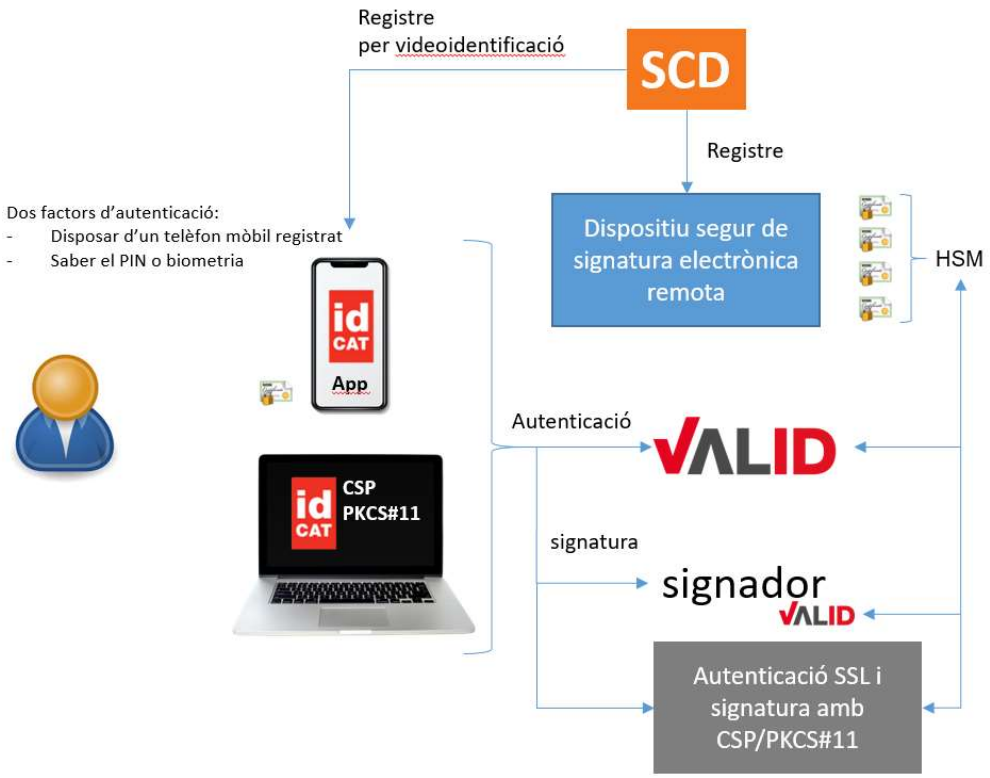

Figura 1. Aplicació Mòbil d'identificació i signatura electrònica

Tal i com mostra l'esquema, l'aplicació mòbil a desenvolupar haurà d'oferir les següents funcionalitats:

- Factor d'autenticació per al servei idCAT Mòbil, que les aplicacions web de les administracions públiques catalanes integren a través del servei VALid per l'autenticació de la identitat de la ciutadania en les seves actuacions en línia.
- Permetre l'obtenció i ús de credencials verificables que el Consorci AOC emetrà en base les fonts de dades personals accessibles a través del servei Via Oberta.
- Factor d'autenticació del servei de signatura remota amb certificats personals que el Consorci AOC ofereix tant als empleats públics i administracions com a la ciutadania.
- Oferir a les aplicacions integrades amb el servei Signador del Consorci AOC la funcionalitat de signatura electrònica amb certificats qualificats des de dispositius mòbils.
- Donar accés als serveis digitals que el Consorci AOC ofereix a la ciutadania

EL desenvolupament de llibreries CSP i PKCS#11 tant per dispositius mòbils com per ordinador queda fora de l'abast d'aquest contracte.

5 Activitats i funcions de l'empresa contractista

Les funcions que ha d'assumir l'empresa contractista són les següents:

- L'empresa adjudicatària serà la responsable de la gestió del projecte i desenvolupament de les aplicacions mòbils objecte del contracte
- Tanmateix serà responsable de la definició del pla de proves d'integració i de rendiment, i de la seu desplegament i execució als entorns de desenvolupament, preproducció i producció.
- Sent responsable del projecte, portarà a terme el control de qualitat i validació del bon funcionament del desenvolupament i 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. o Revisió i seguiment de la qualitat de la documentació generada pels equips de desenvolupament.

6 Requisits generals obligatoris

L'empresa contractista ha de disposar dels suficients mitjans tècnics, materials qualitatius i personals per a desenvolupar les tasques objecte d'aquest contracte.

La prestació regulada en aquest plec ha d'ajustar-se, almenys, als requisits tècnics següents, sens perjudici dels paràmetres que s'han de valorar mitjançant els criteris d'adjudicació establerts.

6.1 Requisits generals obligatoris

6.1.1 Normativa vigent de compliment obligat

- Llei 29/2010, del 3 d'agost, de l'ús dels mitjans electrònics al sector públic de Catalunya
- Reglament (UE) 910/2014 del Parlament i del Consell, de 23 de juliol de 2014, relatiu a la identificació electrònica i els serveis de confiança per les transaccions electròniques en el mercat interior i que deroga la Directiva 1999/93/CE.
- Decisió d'Execució (UE) 2015/1506 de la Comissió, de 8 de setembre de 2015, per la que s'estableixen les especificacions mínimes relatives als formats de signatura avançada i segells avançats que han de reconèixer els organismes del sector públic de conformitat amb l'article 27, apartat 5, i 37, apartat 5, del ReIDAS
- Llei 6/2020, de l'11 de novembre, reguladora de determinats aspectes dels serveis electrònics de confiança
- Ordre ETD/465/2021, de 6 de maig, per la que es regulen els mètodes d'identificació remota per vídeo per l'expedició de certificats electrònics qualificats.
- Llei 39/2015, d'1 d'octubre, de Procediment Administratiu Comú de les Administracions Públiques
- Llei 40/2015, de 1 d'octubre, de Règim Jurídic del Sector Públic. Real decret 203/2021, de 30 de març, pel qual s'aprova el Reglament d'actuació i funcionament del sector públic per mitjans electrònics.
- Reglament (UE) 2016/679, de 27 d'abril del 2016 relatiu a la protecció de les persones físiques pel que fa al tractament de dades personals.
- Esquema Nacional de Seguretat, regulat pel Real Decret 311/2022, de 3 de maig.
- Esquema Nacional d'Interoperabilitat, regulat pel Real Decret 4/2019, de 8 de gener.

6.1.2 Requisits funcionals

En resum, els requisits de la solució seran:

[R1] Es requereix una aplicació mòbil per dispositius tant Android com iOS.

[R2] A nivell funcional i d'arquitectura, les aplicacions objecte d'aquesta licitació s'ajustaran als requisits funcionals i d'arquitectura d'una cartera europea d'identitat digital descrits al document "The Common Union Toolbox for a Coordinated Approach Towards a European Digital Identity Framework – The European Digital Identity Wallet Architecture and Reference Framework", sent aquest el marc de referència per la implementació de carteres d'identitat amb acord al que estableix la proposta de modificació del ReIDAS, actualment en procés d'aprovació.

[R3] Per altra banda, les aplicacions mòbils hauran d'oferir un mecanisme, com a mínim, que pugui ser emprat com a factor d'autenticació per les persones usuàries del servei idCAT Mòbil com a alternativa a l'enviament de paraules de pas d'un sol ús per SMS al propi dispositiu mòbil.

[R4] Les empreses licitadores hauran de disposar d'un prototipus o solució d'aplicació mòbil que es pugui emprar com a mecanisme d'autenticació per l'accés de serveis en línia com a proposta per la seva integració i ús en el servei idCAT Mòbil.

[R5] Com a segon factor d'autenticació, aquest mecanisme haurà de poder garantir un nivell mig de seguretat d'acord amb el que estableix el Real Decret 311/2022, de 3 de maig, que regula l'Esquema Nacional de Seguretat.

[R6] Aquest mecanisme d'identificació electrònica serà el que empraran les persones usuàries del servei idCAT Mòbil a través del servei VALID. L'empresa adjudicatària d'establir els mecanismes que permetran l'ús de l'aplicació mòbil per part d'aquest servei i descriure a la seva proposta les adaptacions que el Consorci AOC haurà de portar a terme per la seva integració.

[R7] Tanmateix, les aplicacions hauran de permetre emprar certificats electrònics qualificats tant en remot, mitjançant el servei que el Consorci AOC proveirà a l'efecte, com en local en processos de signatura electrònica.

[R8] A l'efecte, s'haurà d'integrar amb el servei de signatura electrònica (Signador) per la producció de signatures en format avançat des d'aquest tipus de dispositius. L'adjudicatari haurà de descriure, igualment, les adaptacions que el Consorci AOC haurà de portar a terme per la seva integració.

[R9] Els certificats qualificats gestionats per l'aplicació mòbil seran els emesos pel Consorci AOC com a Prestador de Serveis de Confiança Qualificat.

[R10] Ha de donar accés al procés de registre que el Consorci AOC prepararà per vincular la identitat de la persona amb la seva aplicació mòbil. Aquest procés es podrà portar a terme emprant una credencial ja existent com idCAT Mòbil, o bé mitjançant el procés de videoidentificació que el Consorci AOC ja utilitza per l'obtenció de idCAT Mòbil i certificats qualificats en remot, que compleix amb els requisits establerts per l'Ordre ETD/465/2021.

[R11] Haurà de donar accés als serveis que el Consorci AOC ofereix a la ciutadania, com e-Notum, Representa i el Meu Espai.

[R12] L'aplicació haurà de permetre gestionar i tenir en compte els diferents estats en que es pot trobar el certificat qualificat remot vinculat (emès, suspès o revocat).

[R13] El mateix procés haurà de servir per establir l'aplicació com a mecanisme d'autenticació de la identitat de la persona posseïdora del dispositiu,

[R14] La solució tindrà diverses modalitats d'ús per part de les administracions catalanes, ja sigui com una APP que la ciutadania es podrà descarregar o bé com un SDK que permetrà reutilitzar totes les funcionalitats esmentades per altres APPs del sector públic que ja tenen un gran ús i aporten molt valor.

[R15] Un cop desenvolupades, les aplicacions mòbils hauràn d'estar disponible des de Google Play per a dispositius Android i Apple Store per iPhone.

[R16] La solució haurà de ser multi-idioma: català, castellà i anglès.

6.1.3 Requisits de protecció de dades

El servei objecte del present plec de prescripcions tècniques no implica cap tractament de dades de caràcter personal per part de l'empresa adjudicatària. Tots els serveis de backoffice que tractin amb dades de caràcter personal seran operats pel Consorci AOC de forma directa, assumint aquest tipus de tractaments vinculats als processos d'identificació, signatura electrònica, emissió i validació de credencials verificades.

Tot i això, les aplicacions mòbils que l'adjudicatari proveirà i que seran emprades per la ciutadania si que gestionaran dades de caràcter personal, pel que fa sobretot a la gestió i ús de certificats

digitals i credencials verificables. En aquest sentit l'adjudicatari haurà de tenir en compte la normativa aplicable a l'efecte. En concret:

[R17] 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 pel que fa a les operacions d'identificació, signatura electrònica i gestió del cicle de vida de credencials verificades i certificats digitals, incloent el seu bloqueig, que es portin a terme amb les aplicacions mòbils objecte del present procés de contractació.

[R18] 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).

[R19] L'adjudicatari haurà de fer i revisar anualment, i quan es produeixi alguna modificació en el tractament de les dades, un 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.

[R20] Es requerirà que l'empresa adjudicatària porti a terme un anàlisi de riscos i si s'escau un anàlisi d'impacte de protecció de dades de caràcter i justifiqui la implantació de totes les mesures de privacitat des del disseny i per defecte implantades a l'aplicació per mitigar els riscos pels drets i llibertats dels titulars de les dades que es tractin en l'APP. A l'efecte, es tindran en compte les guies i recomanacions de les autoritats competents en matèria de protecció de dades en compte, com per exemple el document "La privacitat des del disseny i per defecte. Guia per a desenvolupadors" de l'Agència Catalana de Protecció de dades.

[R21] En cas que canviïn els tractaments relatius a dades de caràcter personal, o la categoria d'aquestes dades, caldrà portar a terme un nou anàlisi de riscos o avaluació d'impacte de protecció de dades.

6.2 Funcionalitats mínimes a desenvolupar

La solució a desenvolupar ha de complir amb les següents funcionalitats i requisits:

[F1] Aplicable en processos d'identificació com a factor d'autenticació. Concretament, s'ha de poder utilitzar pels usuaris de l'idCAT Mòbil mitjançant l'enviament de desafiaments push al dispositiu o escanejant codis QR.

[F2] El mètode d'autenticació implementat haurà de poder ser implantat per la verificació la identitat de les persones en processos presencials mitjançant la presentació de l'aplicació mòbil.

[F3] Ha de permetre la vinculació de l'app i el seu ús amb la identitat de la persona usuària. Aquesta vinculació es podrà portar a terme mitjançant un procés de identificació amb una credencial ja existent accessible des del servei VALID del Consorci AOC, o bé mitjançant un procés d'identificació remota de la persona per videoidentificació que compleixi amb els requisits establerts a l'Ordre ETD/465/2021, del 6 de maig, per la que es regulen els mètodes d'identificació remota per vídeo per l'expedició de certificats electrònics qualificats. L'aplicació mòbil objecte de la present licitació haurà de preveure el mecanisme que permeti fer aquesta vinculació, tot i que els procediments concrets seran implementats pel propi Consorci AOC emprant el servei de videoidentificació que actualment ja utilitza per emetre idCAT Mòbil i idCAT Certificat.

[F4] A partir de la identificació remota, la solució ha d'habilitar l'activació de l'APP i gestionar el procés d'obtenció d'un certificat qualificat que es podrà allotjar en remot al servei que el

Consorci AOC disposa, i haurà de tenir en compte tots els estats possibles del seu cicle de vida: emissió, renovació, suspensió, revocació.

[F5] L'aplicació haurà de permetre la signatures electròniques amb aquest certificat.

[F6] També haurà de poder produir signatures electròniques amb certificats qualificats en remot emprant el servei que ofereix el Consorci AOC a l'efecte.

[F7] Utilitzar els mecanismes d'identificació biomètrica del propi dispositiu mòbil per accedir a l'APP i l'ús de les claus i credencials.

[F8] Permetre obtenir, gestionar i compartir credencials verificables d'identitat autogestionada en els processos d'autenticació i tramitació amb les administracions públiques amb acord al que descriu la recomanació *W3C Verifiable Credentials Data Model v1.1*

[F9] Donar accés a la ciutadania als serveis web *responsive* que ofereix el Consorci AOC, per exemple:

- **e-NOTUM:** permet la creació i gestió de les notificacions i comunicacions electròniques dels ens cap a la ciutadania d'una manera senzilla i àgil amb totes les garanties legals i tècniques. Les aplicacions mòbils objecte de la present licitació hauran de poder rebre, acceptar i rebutjar notificacions electròniques amb e-NOTUM, així com consultar les notificacions rebudes.
- **El Meu Espai:** És un lloc web que facilita a la ciutadania conèixer l'estat de les seves gestions i tràmits amb l'Administració d'una manera senzilla, simplifica i integra les actuacions ciutadanes en una visió interadministrativa i posa a disposició les seves dades personals i eines de control de l'ús que en fa l'Administració. Les aplicacions mòbils hauran de donar accés a aquest lloc web, que permetrà l'emissió de credencials verificables gestionades per les mateixes amb acord a les característiques funcionals que ofereixin.
- **Representa:** Representa és un registre electrònic d'apoderaments comú que l'AOC posa a disposició de l'Administració de la Generalitat de Catalunya, les Entitats locals de Catalunya i dels organismes públics i entitats de dret públic vinculats o dependents dels anteriors. Les aplicacions mòbils objecte de la present licitació hauran de permetre crear representacions així com consultar les representacions vinculades a la persona usuària tant com a representant com a poderdant.

La informació concreta dels serveis està disponible al lloc web del Consorci AOC.

6.3 Serveis tecnològics

Les empreses licitadores hauran de descriure els serveis necessaris integrats en les aplicacions mòbils objecte de la seva oferta amb l'objectiu d'assolir els requisits descrits en aquest plec. Aquests serveis poden incloure, per exemple:

- Servei en línia de suport a la gestió del cicle de vida de les credencials verificables
- Servei de suport als processos d'autenticació
- Bus d'integració per les aplicacions usuàries de les aplicacions mòbils
- Qualsevol altre servei necessari per assolir les funcionalitats requerides en aquest plec

En qualsevol cas, caldrà garantir que la integració de les funcionalitats d'aquests serveis manté el la imatge corporativa del Consorci AOC, sent consistent amb l'experiència d'usuari de les aplicacions on s'integri.

7 Formes de seguiment i control de l'execució de les condicions

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 que s'estableixin 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 del servei i/o Cap de Projecte per part del Consorci AOC i personal directiu de l'AOC si s'escau.
- Periodicitat: trimestral.
- Objectiu: fer el seguiment del contracte, analitzant diversos aspectes: productivitat, control d'hores, temes de facturació, seguiment de fites (a alt nivell), etc.
- Lliurables:
    - Informe resum de les actuacions ja resoltes, en curs i pendents, amb el seu grau de priorització.
    - Escandall d'hores totals realitzades en el període amb caràcter mensual.

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 Servei i/o el Cap de Projecte, o algun dels tècnics assignats al projecte.
- Periodicitat: setmanal.
- Objectiu: seguiment del compliment de l'ANS, rendiment de la plataforma, incidències més destacables, i seguiment dels evolutius i correctius a prioritzar.

La comunicació, gestió i dedicació de les tasques, incidències i propostes de millora es realitzarà mitjançant alguna de les següents eines: JIRA (com a eina de negoci i seguiment), Teams i Zendesk del Consoci AOC.

8 Aspectes de seguretat i ENS

El desenvolupament es farà amb els següents requeriments de seguretat per defecte:

[R22] La metodologia de desenvolupament convé que sigui un estàndard reconegut que inclogui la seguretat com a part integral del desenvolupament (per exemple, METRICA, Security Development Lifecycle, Correctness by Construction, Building Security In Centre Criptològic Nacional SENSE CL Maturity Model, OWASP, etc.). És a dir, des de la concepció arquitectònica cal plantejar els requisits de seguretat del sistema final i anar optant per solucions que introdueixin els controls necessaris en el programari desenvolupat.

[R23] Cal evitar que es desenvolupi pensant únicament en la funcionalitat i que els requisits de seguretat s'afegeixin posteriorment.

[R24] Desenvolupament integral significa que les funcions de seguretat són part de la interfície d'usuari, que els registres d'activitat i incidències són part de l'arquitectura de registre i que existeixen mecanismes de validació, protecció de la informació i verificació que es respecta la política de seguretat desitjada.

[R25] Durant les proves de desenvolupament i d'acceptació no es faran servir dades de prova reals, sinó dades específiques per a proves. Quan les dades de prova procedeixin de dades reals, es manipularan perquè no es puguin reconèixer dades reals en les proves. En últim cas, si fos inevitable usar dades reals, es protegiran com si estiguessin en producció. Finalment, les dades de prova s' han de retirar quan el sistema passa a producció.

[R26] La inspecció del codi font ha de ser possible tant durant el desenvolupament com durant la vida útil del programari. Inspeccionar tot el codi és costós i probablement injustificat en els sistemes de suport a l' ENS; però cal accedir al codi font per analitzar incidents i per planificar proves de penetració. Per això ha d' estar disponible amb les degudes garanties de control d' accés.

[R27] En tot cas cal revisar fallades típiques de programació que puguin derivar en problemes de seguretat: desbordament de buffers, informació residual en emmagatzematge temporal (RAM, fitxers en disc, dades a la xarxa, dades al núvol, ...), emmagatzematge de claus i material criptogràfic, validació de les dades d'entrada, d'usuaris i entre processos, validació de la configuració, possibilitats d'injecció de codi, possibles race conditions (carreres de concurrència), escalat de privilegis, comunicacions sense autenticar i/o sense xifrar, etc.