PLEC DE PRESCRIPCIONS TÈCNIQUES

CONTRACTE DE SERVEIS DE DISSENY, DESENVOLUPAMENT I IMPLEMENTACIÓ D'UNA PLATAFORMA AUXILIAR DE TRAÇABILITAT I CADENA DE CUSTÒDIA D'UN SISTEMA DE GESTIÓ D'EVIDÈNCIES DIGITALS

EXPEDIENT: 2025122400

i2CAT Foundation
The Internet Research Centre
C/ Gran Capità 2-4, Edifici Nexus I
2a planta, 08034 Barcelona

Continguts

1. Introducció

1.1. Context

La Fundació i2CAT és un centre de recerca i innovació, fundat l'any 2003 i amb seu a Barcelona, que forma part dels Centres de Recerca de Catalunya (CERCA). L'organització es dedica a dissenyar i construir la societat digital del futur a través del coneixement generat en el desenvolupament d'activitats d'R+D+I en àrees com el 5G/6G, IoT, tecnologies immersives i interactives, ciberseguretat, intel·ligència artificial, cadena de blocs, comunicacions espacials i altres àmbits de la transformació digital.

La Fundació i2CAT participa activament en diversos programes estratègics, que tenen com a finalitat potenciar la innovació digital a Catalunya i la transformació de l'administració pública catalana. Dins d'aquesta estratègia, està impulsant la creació d'un sistema de custòdia digital d'evidències.

En un moment de transformació digital accelerada i d'elevada exposició a les amenaces cibernètiques, la consolidació d'un servei de ciberseguretat que protegeixi de manera efectiva la ciutadania, les empreses i l'Administració esdevé una prioritat estratègica per a Catalunya. Aquesta és, precisament, una de les línies mestres que aposta per desplegar una política pública robusta, orientada a la protecció digital, a la generació de confiança i a la consolidació d'un ecosistema de ciberseguretat avançat i competitiu.

En aquest context, s'identifica la necessitat estratègica de garantir la veracitat, integritat i traçabilitat de les evidències digitals. Per donar resposta als reptes creixents en la preservació, autenticitat i gestió de les evidències digitals, i2CAT impulsa el desenvolupament d'una plataforma avançada de gestió d'evidències digitals (Digital Evidence Management System – DEMS), concebuda com una solució tecnològica integral i d'alta fiabilitat, alineada amb els principis de seguretat per disseny i privadesa per defecte.

Aquesta plataforma proporcionarà un sistema de custòdia i control d'accés a proves digitals, dotat d'un sistema de criptografia avançat, d'última generació, basat en xifrat delegat (proxy re-encryption) i cadena de blocs (blockchain). Això permetrà xifrar les proves i controlar-ne l'accés, de manera que els responsables d'un servei corporatiu no hi tinguin accés en clar, exonerant-los de responsabilitat legal. A més, el sistema generarà un registre d'esdeveniments que permetrà rastrejar totes les accions de la cadena de custòdia.

1.2. Fites i objectius de la licitació

Proporcionar un mòdul específic focalitzat a la normalització d'esdeveniments, proporcionant una capa d'abstracció, habilitant la funcionalitat per a realitzar d'auditories traçables basades en un registre semànticament normalitzat i consistent. Aquest mòdul s'integrarà a la futura plataforma de gestió d'evidències digitals i complementarà les funcionalitats centrals de la plataforma, que

comprenen la implementació de les primitives criptogràfiques necessàries per assegurar un control exhaustiu dels processos de gestió i custòdia d'evidències digitals.

El mòdul a desenvolupar ha de garantir la consistència i la interpretació uniforme de les dades, facilitant l'anàlisi forense, la detecció de possibles anomalies i la gestió d'excepcions. A més, ha de complir amb els estàndards i regulacions pertinents en matèria de seguretat i protecció de dades així com el conjunt de requisits funcionals i tècnics detallats en les subsegüents seccions.

2. Objecte del contracte o necessitat que s'ha de cobrir

Aquesta licitació té com a objectiu la contractació dels serveis necessaris per al disseny, desenvolupament i implementació d'un mòdul específic a integrar-se amb la plataforma de gestió d'evidències digitals, anomenada DEMS (Digital Evidence Management System).

Aquest mòdul s'encarregarà de normalitzar la informació operativa continguda en els registres d'activitat de la plataforma, donant compliment a l'estàndard ISO 22095:20 relatiu a la cadena de custòdia. El mòdul a desenvolupar haurà de ser interoperable amb el servei de traçabilitat de la plataforma DEMS, que proporcionarà un registre verificable d'actuacions operatives mitjançant un registre immutable, dinàmic i programable, basat en contractes intel·ligents i interoperable amb la màquina virtual Ethereum (Ethereum Virtual Machine - EVM)[1].

L'objectiu del servei a contractar contempla les següents activitats:

- Desenvolupament i implementació del mòdul de Cadena de Custòdia i traçabilitat. D'acord al que recull l'estàndard ISO 22095:20[2][3].
- Implementació d'interfícies mitjançant APIs per a integrar-se a la plataforma DEMS per a la normalització d'esdeveniments relacionats amb la cadena de custòdia d'evidències digitals, com son l'obertura d'actuacions, la ingesta d'evidències, la delegació, l'accés i la revocació d'accés.
- Un registre auditable i immutable dels esdeveniments normalitzats processats per la implementació del sistema de normalització al llarg del temps, garantit mitjançant signatures criptogràfiques implementades amb contractes intel·ligents sobre una cadena de blocs compatible amb la màquina virtual d'Ethereum (EVM)[4]. La prescripció tècnica referent a l'ús de la Ethereum Virtual Machine (EVM) es justifica per la necessitat imperativa d'interoperabilitat, estandardització i portabilitat del codi, i no respon a l'elecció d'una marca

[1] Ethereum Virtual Machine (EVM) com a prescripció tècnica justificada per la necessitat d'interoperabilitat i l'ús d'un estàndard tècnic obert i públic (ERC/EIP) de contractes intel·ligents.
[2] La norma ISO 22095:20 és un estàndard obert, publicat i accessible a qualsevol part interessada mitjançant adquisició als organismes de normalització corresponents (ISO/UNE).
[3] El compliment de la ISO 22095:20 és la definició funcional i semàntica de l'objecte del plec (una Cadena de Custòdia Auditable).
[4] Ethereum Virtual Machine (EVM) com a prescripció tècnica justificada per la necessitat d'interoperabilitat

comercial ni d'un producte propietari, garantint així la lliure concurrència. L'EVM actua com un estàndard industrial de facto i una arquitectura de processament de codi obert, definida públicament i implementada per múltiples proveïdors i tecnologies diferents (incloses xarxes públiques, privades i consorciades com Hyperledger Besu o Go-Quorum).

3. Activitats i funcions de l'empresa contractista

L'oferta que presenti l'empresa licitadora ha d'abastar la totalitat de les activitats i funcions especificades en aquest plec i en el plec de clàusules administratives particulars, ja que són totes obligatòries per a l'admissió de les propostes.

3.1. Disseny i anàlisi inicial

Activitats

- **Anàlisi i concreció exhaustiva de les necessitats:** S'analitzaran en profunditat tots els documents de licitació per concretar les necessitats reals del projecte, assegurant una comprensió completa dels objectius i les expectatives.
- **Validació tècnica i funcional:** La proposta tècnica i funcional serà validada rigorosament per garantir que compleix al 100% amb els requisits establerts en la licitació. Aquesta validació assegura que la solució proposada és viable, eficient i alineada amb les necessitats de la plataforma.
- **Definició de l'arquitectura del sistema:** Es definirà l'arquitectura funcional i tècnica del sistema, que inclourà els següents lliurables.

Lliurables

- **Document de validació de requisits:** Document detallat que ha de recollir de manera detallada quins són els requisits mínims desitjables, tant funcionals com tècnics, conjuntament amb criteris d'acceptació específics i mesurables. Això permetrà una avaluació objectiva del compliment dels requisits.
- **Arquitectura tècnica de la cadena de blocs:** Es proposarà una arquitectura tècnica que inclogui la implementació específica de la cadena de blocs, assegurant la compatibilitat amb l'Ethereum Virtual Machine (EVM) per aprofitar les eines i l'ecosistema existents.
- **Especificació d'APIs i fluxos de dades:** S'especificaran detalladament les APIs i els fluxos de dades suportats pel sistema. Aquesta especificació és fonamental per garantir la traçabilitat completa de les transaccions i la realització d'auditories eficients i precises.

3.2. Desenvolupament i integració

Activitats

- Fase d'implementació del codi font, tant dels Contractes Intel·ligents com del Mòdul d'API RESTful / Asíncrona, seguint els Requisits Funcionals (Secció 5.1) i els Requisits Tècnics / No Funcionals (Secció 5.2).

Lliurables

- Els lliurables clau d'aquesta fase (Fases 2 i 3 de la Planificació) inclouen el Codi Font dels Contractes Intel·ligents (C-201) i el Codi Font del Mòdul d'API (C-202), així com la Documentació de l'API (M-402).

3.3. Proves i validació

Activitats

- Inclou la creació i l'execució d'una Suite de Tests d'Integració i Robustesa (STIR) per a l'acceptació final. Es valida la funcionalitat del mòdul, la integritat criptogràfica (AC-F-01), la no-repudiació (AC-F-02) i el compliment dels Requisits No Funcionals (Secció 5.3.3), com la latència màxima de registre de 60 segons (AC-NF-01).

Lliurables

- Els lliurables essencials són el Codi Font de la STIR (T-301) i les Utilitats de Verificació Criptogràfica CLI (T-302). També es lliuren els Informes de Qualitat i Auditories (T-303).

3.4. Desplegament i implementació

Activitats

- Preparació del mòdul per al seu desplegament final, lliurant la configuració necessària per a un entorn de producció. S'exigeix que el mòdul sigui lliurat en un format de contenidor que compleixi amb les especificacions de l'Open Container Initiative (OCI) com per exemple Docker per facilitar el desplegament en entorns al núvol, incloent-hi la infraestructura base de la xarxa EVM permisionada (mínim 3 nodes).

Lliurables

- El lliurable principal és els Arxius de Desplegament per Contenidors (C-203).

3.5. Formació operativa i transferència de coneixement

Activitats

- Lliurament de tota la documentació necessària per al manteniment, la gestió operativa de la xarxa EVM i l'ús dels serveis d'auditoria. Inclou protocols detallats de resolució d'incidències i la gestió del cicle de vida de les claus criptogràfiques.

Lliurables

- Els lliurables (Secció 5.4.4) inclouen el Manual de Manteniment i Operacions (M-401), la Documentació de l'API (M-402) i el Manual d'Usuari dels Serveis d'Auditoria (M-403).

4. Durada del contracte i modalitat d'execució

La durada del present contracte per al disseny, desenvolupament i implementació del Mòdul de Cadena de Custòdia s'estableix en tres mesos i mig naturals a comptar des de la data de signatura de l'acta d'inici del servei.

L'execució d'aquestes activitats es durà a terme mitjançant un model de desenvolupament concurrent amb els treballs d'implementació de la plataforma central DEMS realitzats per la Fundació i2CAT. Aquesta modalitat d'execució es fonamenta en els següents principis:

- **Estructura per fases:** Els treballs s'articulen en les cinc (5) fases de desenvolupament paral·lelitzades detallades a la secció 6.1 d'aquest plec , per tal de garantir que la capa d'immutabilitat evoluciona de forma coordinada amb la lògica de negoci del nucli del sistema.
- **Integració bidireccional:** Atès que el mòdul objecte d'aquesta licitació depèn de dades de la plataforma central (com la identitat corporativa GICAR) i viceversa, el contractista haurà de complir estrictament amb els punts de control d'integració definits per a les setmanes 6, 10 i 18.
- **Gestió del seguiment:** S'establirà una coordinació tècnica i operativa permanent, que inclourà reunions de seguiment amb una periodicitat mínima setmanal entre el/la responsable designat/da pel contractista i la Fundació i2CAT.
- **Lloc d'execució:** Els treballs es duran a terme principalment a les instal·lacions de l'adjudicatari, tot i que es podran preveure sessions de treball presencials o telemàtiques conjuntes per a les tasques de validació de la Suite de Tests d'Integració i Robustesa (STIR).

5. Activitats i funcions de l'empresa contractista

Per assolir els objectius de garantir el disseny, el desenvolupament, la integració i la validació del mòdul específic de normalització i traçabilitat d'esdeveniments en la cadena de custòdia en el context de la plataforma DEMS, d'acord amb la normativa ISO 22095:20, s'ha establert un conjunt de necessitats a satisfer. Aquestes necessitats s'estructuren en tres categories clau: requisits funcionals mínims, requisits funcionals desitjables i requisits tècnics. Per a una comprensió detallada de la planificació temporal i la priorització d'aquests requisits , consulteu l'Annex 1, titulat "Taula de requisits i priorització".

5.1. Requisits funcionals

En aquesta secció es descriuen els requisits funcionals essencials del mòdul a desenvolupar específicament concebut per integrar-se a la plataforma. En concret, s'exposen els diferents elements recollits a la norma ISO 22095:20 i la seva relació amb les entitats i els fluxos de treball suportats per la plataforma. L'objectiu és definir la naturalesa de les interfícies de la implementació del mòdul que es licita.

5.1.1. Introducció i propòsit

5.1.1.1. Definició d'actuació i rols principals

Actuació: Conjunt de procediments duts a terme per una entitat sol·licitant autoritzada per a realitzar, entre altres accions, la recollida d'evidències fora de la plataforma vinculada a l'actuació. Totes les evidències tractades pel sistema han d'estar necessàriament vinculades a una actuació concreta.

Actuant: Entitat autoritzada i legalment responsable de l'actuació en tot moment. L'actuant es defineixi com l'"Organització" responsable última, i el delegat com la persona que exerceix la funció d'Organització/Custodi Administratiu.

Delegat: Organització, usuari o representant identificat pel sistema a efectes administratius com a responsable d'una actuació. Correspon al rol d'actor o organització de la norma ISO 22095:20 i és el custodi, no necessàriament exclusiu, però sí exhaustiu, de totes les evidències recollides en una actuació.

Agent: Perit, forense o entitat encarregada de l'extracció, el tractament i registre de les evidències digitals a la plataforma, d'acord amb els requisits forenses pertinents. També es considera el rol d'actor en termes de la norma ISO 22095:20 pel que fa al tractament d'una o més evidències vinculades a una actuació. L'agent és el responsable de la traçabilitat del seu període de custòdia i de l'ús de mètodes forenses que garanteixin la no alteració (integritat) de l'evidència.

Cal diferenciar el rol administratiu del delegat (responsable de la gestió de l'actuació) i el rol forense de l'Agent (custodi directe i exclusiu de l'evidència digital en el temps). El delegat és la figura de gestió superior que designa (o delega l'accés a la plataforma a) els agents.

Administrador del mòdul de cadena de custòdia: Serà el responsable de la gestió del mòdul i disposarà d'una identitat registrada a la plataforma que assumirà les responsabilitats operatives i de conformitat respecte a la gestió de les identitats vinculades dels diferents agents. Els diferents serveis de consulta d'auditoria i conformitat hauran de presentar les corresponents sortides degudament signades amb la seva clau privada.

Administrador de la plataforma: Responsable de la plataforma DEMS on s'integra el mòdul; totes les crides i integracions amb els serveis del mòdul per part de la plataforma es realitzaran d'acord amb un esquema d'autenticació adient (OAuth 2.0 o API Key robusta) corresponent a aquesta identitat.

5.1.1.2. Model d'identitat preservada

El model de la norma ISO 22095:20 que es considera s'adhereix al model d'identitat preservada. Pel que fa a les evidències, això implica que una entrada específica (una imatge o còpia sòlida des del punt de vista forense) i les seves declaracions associades (p. ex., valor hash, metadades) s'han de mantenir separades i totalment traçables durant tot el procés. S'ha de tenir igualment en consideració la no-alteració del contingut original com a requisit fonamental del model.

5.1.1.3. Model d'esdeveniments de la plataforma

Consideració particular: *Cal destacar que, en l'àmbit d'aquesta plataforma, la delegació d'accés i la transformació del xifrat de les dades del procés de Custòdia s'implementaran mitjançant claus de Proxy Re-encryption. Aquest mecanisme, juntament amb la lògica de delegació corresponent, és gestionat per la capa superior de la plataforma abans de la crida a aquest mòdul d'implementació ISO 22095:20. Així mateix, totes les signatures requerides en el procés de Cadena de Custòdia (tant per la delegació com per la traçabilitat de les accions) es realitzaran utilitzant les claus de signatura de la mateixa plataforma (les quals estan lligades de manera verificable a les identitats dels agents al registre immutable subjacent), i no directament amb les claus natives d'Ethereum. Aquest enfocament garanteix la seguretat criptogràfica de la traçabilitat sense exposar les claus privades Ethereum dels agents pel que fa al mòdul.*

- Col·lecció de l'evidència
    - Prerequisits:
        - Existeix una actuació degudament informada per part d'un actuant que ha designat un delegat d'identitat coneguda.
        - L'agent que executa la col·lecció de l'evidència fora de la plataforma:
            - Ha de disposar d'una d'identitat validada, reconeguda i autoritzada a la plataforma..

- Ha de registrar-les a la plataforma aportant el seu contingut xifrat, un resum criptogràfic dels continguts de l'evidència digital xifrada i contingut en clar.

  - Informació a registrar:
    - Identificador de l'actuació.
    - Identitat de l'agent.
    - Resums criptogràfics (hashos) de l'evidència en clar i xifrada.
    - Marca de temps de l'esdeveniment.
    - Descripció de la font de l'evidència.

- Delegació d'accés (segons ISO 22095:20 - transferència)
  - Prerequisits:
    - L'evidència ja ha estat degudament registrada a la plataforma i al mòdul de cadena de custòdia (1).
    - Existeix un agent d'identitat coneguda que prèviament ha col·lectat l'evidència o ha estat objecte d'una delegació anterior, i que delegarà l'accés a l'evidència a un altre agent.
    - L'agent subjecte de la delegació té identitat coneguda.
    - Existeix una signatura criptogràfica generada per l'agent que delega l'evidència, corresponent al càlcul d'una clau criptogràfica de transformació del xifratge de l'evidència per tal de fer-la desxifrable per part de la clau de l'agent delegat.
  - Informació a registrar:
    - Identificador de l'evidència.
    - Identitat de l'agent delegant.
    - Identitat de l'agent delegat.
    - Signatura per part de l'agent delegant i signatura de la clau criptogràfica de transformació.
    - Propòsit de la delegació xifrat i signat criptogràficament amb la clau de l'agent delegant.
    - Marca de temps de l'esdeveniment.
- Acceptació
  - Prerequisits:
    - Una evidència de la qual ja ha estat registrat un esdeveniment de delegació per part d'un agent delegant a un delegat.
    - L'agent delegat accepta la delegació d'accés.
  - Informació a registrar:

        - Identificador de l'evidència.
        - Identificador del registre de delegació.
        - Signatura criptogràfica per part de l'agent delegat de l'acceptació.
        - Comentaris xifrats per part de l'agent delegat amb la clau de l'agent delegant.
- Accés a una evidència
    - Prerequisits:
        - Un agent d'identitat coneguda amb accés o accés delegat a una evidència registrada.
        - En cas que l'agent hagi estat delegat, la seva acceptació ja ha estat registrada.
    - Informació a registrar:
        - Identificador de l'evidència.
        - Identitat de l'agent que accedeix a l'evidència.
        - Propòsit de l'accés xifrat i signat criptogràficament amb i) la clau de l'agent que accedeix a l'evidència en cas que l'evidència resulti registrada originalment per l'agent o ii) xifrat a la clau de l'agent anterior (delegant) en la cadena de custòdia.
- Revocació d'accés a una evidència
    - Prerequisits:
        - Existeix un agent d'identitat coneguda que ha estat delegat per accedir a una evidència.
        - Existeix un agent d'identitat coneguda que ha delegat l'accés a l'evidència.
        - Efecte de la revocació: Aclareix que la revocació no elimina la traça de Cadena de Custòdia, sinó que tanca el període de custòdia doncs la plataforma ha esborrat la clau d'accés fent que l'Agent ja no pugui accedir al material desxifrat.
    - Informació a registrar:
        - Identificador de l'evidència.
        - Identitat dels agents delegant i delegat.
        - Marca de temps de l'esdeveniment.
        - Motiu de la revocació (finalització de l'anàlisi, baixa de l'Agent, etc.) xifrat i signat criptogràficament amb la clau de l'agent delegant.
- Registre del processament d'una evidència
    - Prerequisits:

- Existeix un agent d'identitat coneguda que té accés (per col·lecció inicial o delegació posterior) a l'evidència en el moment del registre del processament.
- Existeix una evidència registrada que ha estat objecte del processament.
- El processament s'ha dut a terme tot generant una traça d'execució i un resultat o sortida que tindran versions en clar i xifrades a la clau de l'agent processant.
- És important que aquesta traça xifrada contingui els passos realitzats i les eines forenses (amb versió) utilitzades. Això dona compliment al requisit de competència (6.4) i el principi d'audibilitat de les directrius forenses (com les d'ACPO/ISO 27037, que complementen la ISO 22095:20).

- Informació a registrar:
  - Identificador de l'evidència processada.
  - Identitat de l'agent processant.
  - Resum criptogràfic del resultat del processament xifrat i en pla.
  - Resum criptogràfic de la traça del processament xifrada i en pla.
  - Marca de temps de l'esdeveniment de registre.
- *Cal destacar que el resultat del processament s'ha de tractar, pel que fa a la resta d'esdeveniments, com una evidència més.*

5.1.1.4. Principis de Seguretat Criptogràfica i Transparència

El mòdul de Cadena de Custòdia s'estructurarà sobre principis de robustesa criptogràfica i transparència.

Funcions Criptogràfiques i Conformitat:

Les funcions criptogràfiques de signatura i validació suportades pel mòdul es basaran en l'algorisme estàndard ECDSA amb corba secp256k1, d'acord amb la implementació nativa de la Màquina Virtual Ethereum. Aquesta aproximació compleix els requisits d'integritat i no-repudiació tècnica de la Cadena de Custòdia. Es prioritzarà l'ús de programari de codi lliure auditat o altament auditable per a totes les dependències i llibreries criptogràfiques clau, garantint la màxima transparència i confiança en els processos de generació de hashes, signatura i, si s'escau, de generació de nombres pseudoaleatoris criptogràficament segurs (CSPRNG) requerits per a qualsevol funcionalitat interna.

Política de Gestió de Claus Privades:

El mòdul està pensat per operar sota un model de custòdia externa de clau privada per maximitzar la seguretat i la no-repudiació. Amb l'única excepció de la identitat de l'Administrador del mòdul de cadena de custòdia, el mòdul no ha d'emmagatzemar, gestionar, ni tan sols tenir accés, a cap clau privada de l'Actuant, del Delegat o dels Agents. La clau privada de l'Administrador del mòdul, que s'utilitza exclusivament per signar els informes d'auditoria i les transaccions de gestió d'identitats,

ha de ser custodiada de manera segura per la plataforma DEMS hoste. És d'obligat compliment el següent requisit. Aquesta custòdia es realitzarà amb mecanismes de protecció de clau forta, d'acord amb el nivell de risc d'una clau mestra del sistema, com poden ser mitjançant la utilització d'un Mòdul de Seguretat de Maquinari (HSM) o un sistema de gestió de claus validat, garantint que la clau privada mai es trobi desprotegida a l'entorn del mòdul.

5.1.2. Gestió d'identitat i persistència

Aquesta secció descriu les característiques funcionals que ha de suportar el mòdul pel que fa a la persistència dels registres d'evidències detallats a les seccions anteriors. Es posa especial èmfasi a la necessitat de mantenir un registre auditable segur i traçable de la cadena de custòdia d'evidències, d'acord amb la norma ISO 22095:20. Aquest registre ha de ser robust criptogràficament, de manera que la informació associada als esdeveniments, un cop consolidada, sigui immutable. Aquest aspecte es considera fonamental i per garantir la integritat i la fiabilitat de les evidències.

5.1.2.1 Arquitectura de Registre Distribuït

Per garantir al màxim la interoperabilitat, la capa inferior d'aquest registre haurà d'estar suportada per tecnologia compatible amb la Màquina Virtual Ethereum (EVM), d'acord amb les seves interfícies comunes i establertes. L'emmagatzemament de la informació en aquesta capa de persistència només inclourà les metadades d'esdeveniments (hashes, marques de temps, signatures, etc.) de la Cadena de Custòdia, mentre que les dades xifrades de l'evidència s'emmagatzemaran a la capa de persistència de la plataforma. Això inclou la capacitat de desplegar contractes intel·ligents programats en Solidity i compilats amb un compilador suportat. En termes generals, s'acceptarà qualsevol implementació de client del protocol d'Ethereum, amb la particularitat que estigui enfocada a una xarxa permisionada amb un mínim de 3 nodes.

Durant l'execució del projecte, l'organització subjecte a licitació mantindrà l'operativa de la xarxa, a més de proporcionar facilitats d'accés segur a aquesta infraestructura base per part d'i2CAT a efectes d'integració. A més de la infraestructura base (xarxa EVM i les seves APIs de servei) es valorarà igualment el desplegament d'un explorador de blocs que faciliti les tasques de depuració i integració. Aquest servei inclourà un compromís de servei i atenció d'incidències intra-diari del 95% del transcurs del projecte en horari laboral central europeu de 9 a 17 hores. Aquest compromís assegurarà una resposta ràpida i eficient a qualsevol problema que pugui sorgir durant el projecte.

5.1.2.2. Definició dels Registres

D'acord amb el model d'esdeveniments especificat a la secció 5.1.1.3, es deixa llibertat en la implementació concreta del contracte o contractes intel·ligents, així com les dependències i interfícies que ha de suportar el programari desenvolupat amb Solidity. Aquesta flexibilitat permetrà a l'equip de desenvolupament adaptar la solució a les necessitats específiques del projecte. A efectes de facilitar la traçabilitat el(s) contracte(s) intel·ligent(s) ha(n) de poder emetre

un esdeveniment per a cada esdeveniment de Cadena de Custòdia definit, i que el hash de l'esdeveniment i la identitat del signant formin part dels paràmetres immutables del registre.

5.1.2.3. Mecanismes de Consens i Prova de Marca de Temps

Els mecanismes de consens i acceptació dels registres, d'acord amb l'estipulat a la secció 5.1.1.3, s'hauran de dur a terme sobre la cadena de blocs d'acord amb l'algoritme de consens entre els nodes. Aquest algoritme ha de ser escalable fins a un màxim teòric de 24 nodes, amb una probabilitat estadística de confirmació de registre que no superi un marge de 60 segons per operació. Aquesta velocitat de confirmació és important per garantir que les evidències es registrin de manera oportuna.

5.1.3. Gestió d'identitats i no-repudiació

El mòdul gestionarà la identitat dels usuaris (agents i delegats) associant-la a les claus públiques. Aquestes claus s'utilitzaran per a dues funcions diferenciades: una per xifrar i signar les evidències per part de la plataforma DEMS (garantint-ne la confidencialitat i autenticitat), i l'altra per transaccionar amb el contracte intel·ligent de la Màquina Virtual Ethereum (EVM) pel que fa al mòdul de Cadena de Custòdia. En l'àmbit del contracte intel·ligent, el mòdul proveirà les funcionalitats necessàries per vincular de forma verificable les identitats reconegudes de la plataforma amb les claus públiques compatibles amb l'EVM, que permet el reconeixement i l'autorització de les accions de registre d'esdeveniments. Això assegurarà que cada pas en la cadena de custòdia estigui clarament associat a un usuari identificat. Pel que fa a la seguretat, la custòdia de les claus privades (utilitzades per signar les transaccions) es realitzarà de forma externa. Les sol·licituds de registre, en forma de transaccions cap als contractes intel·ligents, seran operacions degudament signades que entraran al sistema. Aquesta gestió externa de les claus privades reforça la seguretat, ja que el mòdul de Cadena de Custòdia no les emmagatzema directament.

5.1.3.1. Gestió del Cicle de Vida de les Claus Criptogràfiques

El mòdul haurà d'implementar totes aquelles funcionalitats derivades del cicle de vida de les claus criptogràfiques de transacció a la infraestructura, incloent:

- Registre d'una clau pública vinculada a una identitat a la plataforma.
- Revocació d'una clau pública.
- Rotació d'una clau pública vigent sota demanda del custodi de la clau privada. Aquestes funcionalitats són essencials per mantenir la seguretat i la integritat del sistema.

5.1.3.2. Vinculació Rol-Identitat-Clau (PKI)

El mòdul inclourà un servei de tipus CRUD (Create, Read, Update, Delete) que permetrà a l'administrador del mòdul de cadena de custòdia amb permisos d'administració pel que fa a la cadena de blocs (e.g., desplegament, gestió de membres/nodes si cal, i el CRUD del registre d'identitats) registrar l'associació d'una clau pública de transacció amb el registre de cadena de

custòdia a una identitat reconeguda a la plataforma, així com les operacions de consulta, actualització de dades i eliminació. Aquest servei permetrà gestionar de manera eficient les associacions entre rols, identitats i claus.

Camps crítics de la identitat reconeguda (DNI, nom, etc.) per a la CdC.

Els camps crítics a tractar per cada usuari, es determinaran d'acord amb refinament dels requisits durant l'execució de la implementació; de manera que es preveu que es pugui suportar el tractament, amb dades fictícies i a títol orientatiu a efectes de desenvolupament, entre d'altres:

- Nom
- Identificador
- Adreça de correu electrònic
- Identificador en el context de l'organització
- Dades de contacte

5.1.3.3. Estàndards de Signatura i Verificació

Els estàndards de signatura i verificació per part dels contractes intel·ligents inclosos com a part de l'arquitectura del mòdul hauran de ser interoperables i compatibles amb les signatures digitals suportades de forma nativa per Ethereum. Això garanteix que el sistema pugui interactuar amb altres sistemes que utilitzen Ethereum.

5.1.4. Funcionalitats operatives i de traçabilitat

Aquesta secció descriu quines són les funcionalitats requerides per a assegurar la interoperabilitat amb el mòdul de custòdia, i garantir una correcta integració amb la plataforma DEMS. També, recull quines són les tipologies d'interfícies que cal suportar per a gestionar el registre d'esdeveniments del model (serveis d'ingrés de dades), així com el conjunt de consultes operatives necessàries per recuperar registres anteriors de manera àgil i eficient. El registres d'esdeveniments no hauran d'estar únicament vinculats a processos d'auditoria i conformitat. L'objectiu és permetre un accés ràpid i fàcil a la informació necessària per al funcionament diari de la plataforma.

5.1.4.1. Serveis d'Ingrés de Dades

El servei d'ingrés de dades donarà suport al registre dels esdeveniments especificats a la secció 5.1.1.3, tal com s'ha esmentat a la secció 5.1.3. A més, acceptarà, com a part de les entrades, les transaccions ja signades per a la seva inscripció a la cadena de blocs (blockchain).

Per garantir la fiabilitat i l'escalabilitat del sistema, aquest servei ha de ser d'índole asíncrona i basar-se en un sistema intermediari robust i fiable de fluxos de dades. Aquest sistema intermediari permetrà una comunicació eficient entre les aplicacions que generen i processen la informació de manera contínua.

En particular, pel que fa al registre d'evidències, el servei ha d'oferir un sistema de canalització adequat per gestionar asíncronament les diferents sol·licituds de la plataforma. Un cop

completada o fallida una operació, el servei ha de proporcionar una resposta clara i inequívoca. Aquesta resposta ha d'indicar l'èxit de l'operació o, en cas de fallida, un missatge d'error específic que concreti de forma il·lustrativa i categoritzada el motiu de l'error o excepció. Aquest sistema de notificacions d'errors ha de ser complet i permetre la resolució ràpida dels problemes.

5.1.4.2. Consultes Operatives a Suportar

El mòdul suportarà una interfície síncrona de consulta operativa per facilitar la integració amb la plataforma. Aquesta interfície es basarà, orientativament, en una API que segueixi el paradigma REST amb funcions de paginació per paràmetres per les consultes exhaustives. La API permetrà:

- Gestió d'identitats registrades (CRUD) PKI: Crear, Llegir, Actualitzar i Eliminar informació relacionada amb les identitats registrades mitjançant una infraestructura de clau pública (PKI).
- Consulta d'actuacions: Permetre la recuperació d'informació sobre actuacions concretes realitzades dins del sistema.
- Consulta d'evidències: Facilitar l'accés a la informació relativa a evidències registrades.
- Consulta d'esdeveniments de la cadena de custòdia: Permetre la recuperació d'informació sobre els esdeveniments registrats a la cadena de custòdia, segons el model especificat a la secció 5.1.1.3. Això inclou el tipus d'esdeveniment, la data i hora, les parts involucrades i els detalls rellevants.
- Consulta de l'històric d'esdeveniments relacionats amb la gestió d'identitats registrades (PKI) incloent: registre, modificació de dades, claus públiques, revocacions, rotacions, etc.

5.1.5. Funcionalitats d'auditoria i conformitat

Aquesta secció defineix les especificacions funcionals del mòdul de gestió de la cadena de custòdia, específicament pel que fa a la generació i presentació d'informes agregats per evidenciar el compliment normatiu, així com a l'auditoria de la cadena de custòdia i de les diferents actuacions registrades. Per garantir la integritat i la traçabilitat en la presentació de resultats, totes les consultes detallades en aquesta secció seran signades criptogràficament amb la clau privada de l'administrador del mòdul de cadena de custòdia. Aquesta signatura assegurarà que els agregats obtinguts no han estat alterats posteriorment a la seva extracció i validació.

5.1.5.1. Ontologia semàntica de cadena de custòdia

Per tal de garantir la comprensibilitat, l'auditabilitat independent i la interoperabilitat semàntica de la Cadena de Custòdia Digital (DCoC) un cop extreta de la plataforma, tots els resultats presentats pels serveis d'auditoria i conformitat (seccions 5.1.5.2, 5.1.5.3 i 5.1.5.4) han de ser autocontinguts semànticament.

Això implica que les dades serialitzades han de complir els següents requisits:

1) **Model de Dades Semàntic:** La serialització de tots els esdeveniments, rols, identitats, hashes i signatures es realitzarà en un format de dades vinculades (Linked Data) compatible amb ontologies semàntiques (preferentment JSON-LD).

2) **Definició Ontològica:** Es definirà una ontologia semàntica de Cadena de Custòdia que permeti als verificadors externs entendre la relació formal entre les entitats del mòdul (Actuació, Evidència, Agent, Delegació, Signatura, etc.) sense requerir el coneixement intern de la base de dades del mòdul.
    a) S'utilitzaran i s'estendran, si escau, ontologies RDF (Resource Description Framework)[5] i definicions de RFC existents per a conceptes genèrics (com marques de temps, identificadors únics o signatures), i es desenvoluparà una ontologia específica del mòdul per als conceptes únics de la Cadena de Custòdia digital i els rols definits al 5.1.1.1.
3) **Verificabilitat Criptogràfica:** L'ontologia haurà d'incloure la definició formal dels mecanismes de verificació de signatures (Signature Suites) i dels algorismes de hashing utilitzats (ECDSA secp256k1, SHA-256)[6], fent explícita la dependència de les claus públiques dels agents.
4) **Autoconteniment Semàntic:** Els arxius de sortida (en format JSON-LD o alternativament en altre format de dades no propietari i llegible per màquina àmpliament acceptat pels estàndards del W3C) han d'incloure els contextos semàntics (schema) necessaris per ser interpretats per qualsevol processador de dades vinculades, assegurant així que el significat de les dades sigui plenament comprensible i auditable fora del context de la plataforma.

5.1.5.2. Funcionalitats d'Auditoria d'Evidència

Es proporcionarà un servei de recuperació exhaustiva de tota la informació associada a una evidència específica, implementat amb paginació per gestionar grans volums de dades. Aquest servei exposarà una interfície RESTful que permeti recuperar de forma cronològica tots els esdeveniments registrats segons el model descrit a la secció 5.1.1.3, serialitzats en un format estàndard serialitzats en format JSON-LD, d'acord amb l'Ontologia semàntica de Cadena de Custòdia (5.1.5.1). Cada registre d'esdeveniment inclourà tota la informació criptogràfica necessària per verificar les signatures de les transaccions de forma independent a la plataforma. A més, el resultat complet de la consulta serà signat amb la clau privada de l'administrador del mòdul per garantir la seva autenticitat.

Per facilitar l'auditoria, es proporcionarà el codi font auditable d'una utilitat de línia de comandes, compatible amb sistemes operatius de Programari Lliure i Obert (FOSS) amb entorn de línia de comandes, com ara GNU/Linux qualsevol equivalent tècnic que garanteixi la màxima transparència i

[5] Tant RDF com JSON-LD són estàndards internacionals i oberts del W3C per a l'intercanvi de dades semàntiques. Garanteixen l'auditabilitat independent i la validesa de les evidències, que permet que qualsevol auditor extern pugui interpretar l'estructura de dades (Ontologia Semàntica) de la Cadena de Custòdia sense estar lligat a la plataforma.

[6] La menció d'ECDSA secp256k1 i SHA-256 no implica cap mena de preferència per un fabricant o proveïdor concret, ni es pretén restringir la concurrència competitiva. ECDSA, SHA-256 i la corba secp256k1 són algorismes i corbes criptogràfiques àmpliament estandarditzades i disponibles en múltiples implementacions de codi obert i biblioteques de programació, subjectes a revisions públiques i utilitzades extensament en la indústria.

audibilitat del codi. Aquesta utilitat permetrà la verificació fora de línia de la validesa del resultat de la consulta, així com la verificació de les signatures de les transaccions. La verificació es realitzarà utilitzant les claus públiques dels agents implicats en cada esdeveniment i la clau pública corresponent a la clau privada de l'administrador del mòdul; la seva funció principal serà interpretar l'estructura JSON-LD i, després, realitzar la verificació criptogràfica. Això permetrà una auditoria independent i transparent.

5.1.5.3. Funcionalitats d'Auditoria d'Actuació

Es contemplen dues funcionalitats lligades a la realització d'auditories d'actuació:

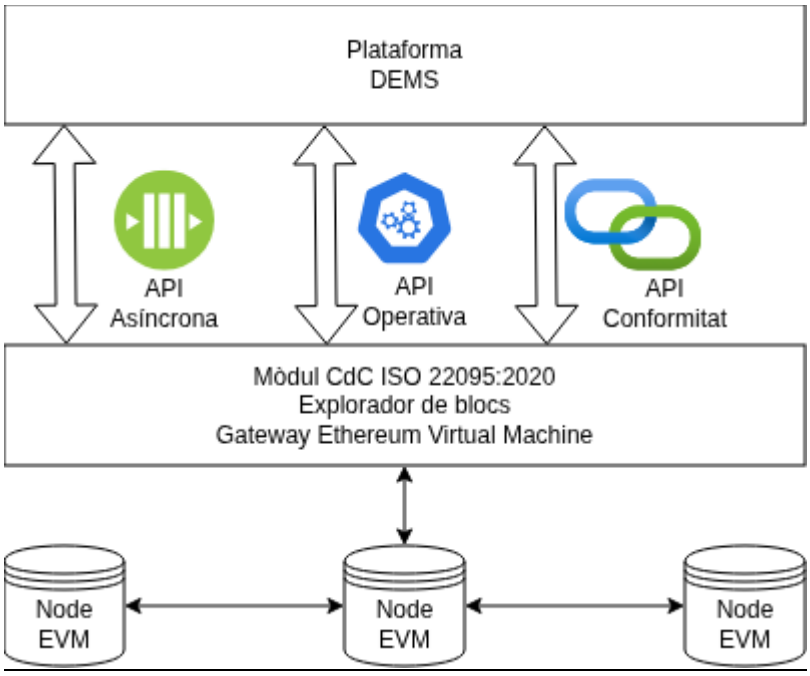
Auditoria d'evidència: Consisteix a proveir un servei per a recuperar de manera escalable i paginada la informació registrada de totes les evidències (descrites a la secció 5.1.5.1) que estiguin vinculades a una actuació determinada.

1. **Verificació externa d'evidències:** Similar a l'auditoria d'evidència, aquesta permetrà la verificació fora de línia dels esdeveniments registrats, tant des del punt de vista formal (estructura de les dades) com criptogràfic (validesa de les signatures). La seva funció principal serà interpretar l'estructura JSON-LD i, després, realitzar la verificació criptogràfica, per fer-ho possible es proporcionarà el codi font auditable, mitjançant línia de comandes compatible amb sistemes GNU/Linux.

5.1.5.4. Generació d'Informes de Conformitat

Aquest servei proporciona informes agregats i resumits basats en les dades recuperades pels serveis descrits a les seccions 5.1.5.1 i 5.1.5.2. Aquests informes seran signats amb la clau privada de l'administrador del mòdul per garantir la seva autenticitat. En lloc d'incloure les signatures detallades de les transaccions individuals de consolidació d'esdeveniments a la cadena de blocs, els informes contindran el resultat de la verificació duta a terme pel servei per a cada registre. Això simplifica la verificació pel que fa a l'informe, proporcionant una visió consolidada i verificada del compliment.

Incloure traçabilitat del procés de gestió de claus de transacció (alta, revocació, rotació, etc.) en forma de events dels contractes intel·ligents.



5.2. Requisits tècnics / no funcionals

5.2.1. Requisits de Rendiment i Capacitat

5.2.1.1. Latència de Registre

El temps màxim mitjà per a la confirmació d'un esdeveniment de CdC (des de l'enviament de la transacció fins a la seva inclusió en un bloc confirmat) no ha de superar els 10 segons en condicions de càrrega normal.

5.2.1.2. Escalabilitat

La infraestructura EVM i els contractes intel·ligents han de ser capaços de suportar un pic teòric de 6 transaccions de CdC per minut (TPM) per un període sostingut de 30 minuts.

5.2.1.3. Capacitat d'Emmagatzemament

El disseny del contracte intel·ligent ha d'optimitzar el consum de "gas" i la necessitat d'emmagatzemar estats, utilitzant la blockchain només per a l'evidència de la CdC (hashes i metadades) i no per a l'emmagatzemament de grans volums de dades.

5.2.1.4. Temps de Consulta

La latència de resposta dels serveis d'auditoria (5.1.5.2 i 5.1.5.3) no ha de superar els 10 segons per a consultes que retornin fins a 100 registres d'esdeveniments.

5.2.2. Requisits d'Arquitectura i Desenvolupament

5.2.2.1. Tecnologies de Programació

Stacks de desenvolupament admissibles (p. ex., Back-end en Python/Django, Node.js/Express; Contractes Intel·ligents en Solidity, etc.).

5.2.2.2. Estandardització de Contractes

El codi dels contractes intel·ligents ha de complir amb els estàndards ERC o qualsevol EIP rellevant per a la lògica de registre (per exemple, per a la gestió d'identitats), preferentment adoptant dependències conegudes i auditades com OpenZeppelin.

5.2.2.3. Qualitat del Codi i Cobertura

Requisit d'entrega del codi font amb un mínim de 90% de cobertura de tests unitaris/integració i un informe d'anàlisi de seguretat estàtica per a tots els contractes Solidity.

5.2.2.4. Ús de codi font obert

Tant el mòdul com les seves dependències principals han de ser open source (o proveir el codi font) per a la seva auditoria.

5.2.3. Requisits de Seguretat

5.2.3.1. Seguretat del Node de Firma

Els nodes de la xarxa EVM responsables de validar i incloure transaccions han d'estar configurats amb polítiques de seguretat de xarxa (ACLs) estrictes, limitant l'accés només a l'Administrador del Mòdul i a la passarel·la d'integració.

5.2.3.2. Auditories de Contractes

Es requerirà un informe d'auditoria de seguretat per a tots els contractes intel·ligents desplegats, abans de la posada en producció.

5.2.3.3. Control d'Accés al Mòdul

El mòdul ha d'implementar un control d'accés per a l'accés a les API de consulta, assegurant que només els usuaris autoritzats (p. ex., Administrador del mòdul o del DEMS) puguin accedir a les dades d'auditoria.

5.2.4. Requisits de Desplegament i Manteniment

5.2.4.1. Desplegament en Contenidors

El mòdul de CdC ha de ser lliurat en contenidors OCI com per exemple Docker per facilitar el desplegament en entorns de producció al núvol.

5.2.4.2. Documentació Tècnica

L'entrega inclourà documentació completa de l'API (Swagger/OpenAPI/AsyncAPI), diagrama d'arquitectura, i instruccions de manteniment de la xarxa EVM.

5.2.4.3. Suport

Durant la implementació, i especialment durant les tasques de desplegament i integració corresponents, es requerirà capacitat de suport durant l'horari d'oficina CET, segons necessitats. El temps de resposta per a consultes relatives a la implementació i/o l'arquitectura no serà superior a dos dies laborals. Per a consultes sobre integració, desplegament i configuració, el temps de resposta no serà superior a un dia laboral. Un cop lliurada i acceptada la implementació, es requerirà un període de suport addicional d'un any natural per resoldre consultes i corregir deficiències.

5.3. Requisits tècnics generals obligatoris de la prestació i/o rendiment o exigències funcionals de la prestació

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

La validació i l'acceptació final del mòdul de Cadena de Custòdia es realitzarà mitjançant l'execució i l'aprovació d'una Suite de Tests d'Integració i Robustesa desenvolupada conjuntament durant el projecte. Tots els tests d'aquesta suite s'han de completar amb el resultat Passa (o 100% de conformitat) per a l'acceptació del mòdul.

5.3.1. Configuració i Abast de la Simulació

La suite es realitzarà mitjançant una simulació paramètrica de l'activitat de la plataforma que compleixi els següents mínims:

Paràmetre de la simulació	Qualitat mínima del test	Criteri d'avaluació
Actuacions Concurrents	10 Actuacions (simultànies)	Prova la separació lògica de la CdC per actuació.
Agents per Actuació	5 Agents diferents (per cada	Prova la correcta vinculació i

	actuació)	gestió de rols.
Evidències Col·leccionades	50 Evidències digitals totals (5 per actuació de mitjana)	Prova la funcionalitat de Col·lecció
Esdeveniments de CdC (total)	Mínim 250 esdeveniments (Col·lecció, Delegació, Acceptació, Processament, Revocació, Accés) registrats.	Prova la cobertura total del Model d'Esdeveniments.

5.3.2. Criteris d'Acceptació Funcional (Passa / No Passa)

Tests destinats a avaluar la correcta implementació dels rols, esdeveniments i l'ontologia semàntica.

Identificador	Test funcional	Criteri d'èxit
AC-F-01	Integritat Criptogràfica	El mòdul ha de registrar i verificar correctament el hash de totes les 50 evidències. **Resultat**: La verificació posterior del hash de l'evidència amb l'eina de línia de comandes (5.1.5.2) coincideix amb el hash registrat a la blockchain per al 100% dels casos.
AC-F-02	No-Repudiació de Delegació	Prova la Delegació i l'Acceptació d'accés (5.1.1.3 - 2 i 3). **Resultat**: L'agent delegant i el delegat són verificables mitjançant les seves signatures privades en el 100% de les 50 transaccions de Delegació i Acceptació.
AC-F-03	Traçabilitat Semàntica	Prova la correcta serialització dels resultats d'auditoria. **Resultat**: L'extracció de l'històric de qualsevol evidència (5.1.5.2) retorna el registre complet en format JSON-LD vàlid i que s'ajusta al 100% a l'Ontologia Semàntica de CdC (5.1.5.1).
AC-F-04	Consistència d'Auditoria	Prova la funció d'Auditoria d'Actuació (5.1.5.3). **Resultat**: La funció d'Auditoria d'Actuació retorna el conjunt complet i exclusiu de les 5 evidències vinculades a qualsevol de les 10 actuacions simulades.
AC-F-05	Signatura d'Auditoria	Prova la no-repudiació dels informes oficials. **Resultat**: Els informes d'Auditoria d'Evidència i Conformitat són verificables amb la clau pública de l'Administrador del Mòdul per al 100% dels casos, sense error tot fent ús de les utilitats de verificació fora de línia descrites a 5.1.5.2 i 5.1.5.3.

5.3.3. Criteris d'Acceptació No Funcionals (Passa / No Passa)

Identificador	Test no funcional	Criteri d'èxit
AC-NF-01	Rendiment (Latència)	Prova el temps màxim de registre de la transacció. **Resultat**: El temps de confirmació (Tx Time) per a qualsevol dels 250 esdeveniments, sota la càrrega concurrent de 10 TPM, no supera els 60 segons.
AC-NF-02	Immutabilitat i Integració EVM	Prova la persistència de les dades. **Resultat:** Cap registre d'esdeveniment a la *blockchain* pot ser alterat o eliminat. El mòdul ha de detectar i rebutjar qualsevol intent d'esborrat o modificació d'una transacció de CdC prèviament confirmada.
AC-NF-03	Inaccessibilitat de Claus Privades	Prova la política de gestió de claus. **Resultat**: Es demostrarà mitjançant revisió de codi i d'infraestructura que la clau privada de l'Administrador del Mòdul està custodiada en el sistema de gestió de claus de la plataforma, i que cap clau privada d'Agent, Delegat o Actuant s'emmagatzema al mòdul.
AC-NF-04	Requisit de Rols	Prova el sistema d'autorització. **Resultat**: El mòdul rebutja amb èxit qualsevol intent de registrar un esdeveniment per part d'un Agent o Delegat la clau pública del qual hagi estat prèviament revocada (simulació de la funcionalitat 5.1.3.1) o no estigui registrada.

5.3.4. Metodologia de Validació

1) **Desenvolupament de la Suite:** El codi de la Suite de Tests (STIR) serà desenvolupat i entregat pel licitador al client (X setmanes) abans de la data d'acceptació final.
2) **Entorn d'Execució:** La suite s'executarà en un entorn de proves que repliqui la xarxa EVM permisionada i la infraestructura base (mínim 3 nodes).
3) **Aprovació:** L'acceptació final només es donarà quan el registre de la Suite mostri un resultat de Passa (100% d'èxit) en tots els tests llistats anteriorment.

5.4. Lliurables

5.4.1. Documents d'especificació i disseny

Identificador	Lliurable	Descripció
D-101	Especificació Funcional i No Funcional (Final)	Document que conté totes les seccions (5.1 a 5.3) acordades, incloent-hi la definició de rols, el model d'esdeveniments, la política de claus i els requisits tècnics/no funcionals (rendiment, seguretat).
D-102	Document d'Arquitectura Tècnica	Descripció detallada de l'arquitectura de la solució, incloent-hi: diagrames d'alt i baix nivell, flux de dades criptogràfiques (xifrat/signatura), i la topologia de la xarxa EVM (nodes, consens).
D-103	Especificació de l'Ontologia Semàntica (JSON-LD)	Document que defineix formalment l'Ontologia Semàntica de Cadena de Custòdia (5.1.5.1), incloent-hi l'esquema JSON-LD, la definició de termes i les relacions ontològiques de tots els esdeveniments i entitats.
D-104	Pla de Gestió de Claus i PKI	Document que detalla la implementació de la política de custòdia de claus (5.1.1.4), els procediments per al cicle de vida de les claus criptogràfiques, i els requisits d'integració amb l'HSM/sistema de gestió de claus de l'Administrador del Mòdul (AC-NF-03).

5.4.2. Codi Font del Mòdul i Contractes

Identificador	Lliurable	Descripció
C-201	Codi Font dels Contractes Intel·ligents	Codi font complet dels contractes Solidity (o equivalent) que implementen el registre immutable de la CdC (incloent-hi el registre d'esdeveniments i la gestió d'identitats/rols), amb el 100% de la cobertura de codi verificable.
C-202	Codi Font del Mòdul d'API RESTful / Asíncrona	Codi font complet dels serveis d'interfície (API) que orquestren les transaccions a la blockchain (Registrar Col·lecció, Delegar Accés, Accedir, etc.) i que suporten les consultes operatives (5.4.2).
C-203	Arxius de Desplegament Contenidoritzat	Configuracions de contenidors (p. ex., Dockerfiles) i arxius de gestió d'infraestructura (p. ex., Docker Compose, manifestos Kubernetes) per al desplegament del mòdul d'API i la xarxa EVM permisionada.

5.4.3. Eines d'Auditoria i Verificació (Fase de Validació)

Identificador	Lliurable	Descripció
T-301	Suite de Tests d'Integració i Robustesa	Codi font complet de la suite de tests automatitzada (5.3) que simula la càrrega paramètrica d'actuacions i agents concurrents, amb tots els tests de verificació funcional i no funcional (latència, no-repudiació).
T-302	Utilitats de Verificació Criptogràfica (CLI)	Codi font auditable de les eines de línia de comandes (GNU/Linux) que permetin la verificació off-chain de la integritat criptogràfica (hashos i signatures d'agents/administrador) i la validació de la sintaxi JSON-LD de les sortides d'auditoria (5.1.5.2).
T-303	Informes de Qualitat i Auditories	Resultats de l'execució de la Suite (Passa/No Passa), informe d'anàlisi de seguretat estàtica del codi Solidity i l'informe de cobertura de tests unitaris (5.2.2.3).

5.4.4. Documentació d'Usuari i Manteniment

Identificador	Lliurable	Descripció
M-401	Manual de Manteniment i Operacions	Guia per a l'Administrador del Mòdul de CdC sobre la gestió operativa (SLA), la monitorització de la xarxa EVM, la resolució d'incidències i els procediments de rotació i revocació de claus.
M-402	Documentació de l'API (Swagger/OpenAPI/AsyncAPI)	Documentació tècnica completa i interactiva de les interfícies RESTful així com les asíncrones amb AsyncAPI del mòdul, facilitant la integració amb la plataforma DEMS hoste.
M-403	Manual d'Usuari dels Serveis d'Auditoria	Guia per a l'ús de les funcionalitats d'Auditoria d'Evidència i Actuació (5.1.5.2, 5.1.5.3) i la interpretació dels Informes de Conformitat (5.1.5.4) per part d'auditors externs.

6. Planificació i terminis d'execució

El desenvolupament del Mòdul de Cadena de Custòdia (CdC) es preveu amb una duració de 3,5 mesos naturals des de la signatura del contracte. El pla s'articula en cinc (5) Fases principals, paral.lelitzades, amb èmfasi en la validació inicial de la capa EVM i la integració amb la plataforma DEMS.

6.1. Fases i fites clau

Fase (Més)	Durada	Punt de control	Objectiu
Fase 1: Disseny i Arquitectura	0.5 Mesos	PC-1: Aprovació de l'Arquitectura.	Fixar l'ontologia semàntica, el disseny dels contractes intel·ligents i els mecanismes de xifrat/custòdia de claus.
Fase 2: Implementació EVM i Identitats	1 Mes	PC-2: Desplegament de la Capa d'Immutabilitat	Desplegament dels contractes intel·ligents bàsics (Registre de CdC i Gestió d'Identitats) a la xarxa EVM de proves i entrega del primer mòdul d'API.
Fase 3: Integració Funcional	1 Mes	PC-3: Integració Bidireccional amb DEMS	Implementació de totes les rutes de l'API (5.4.1) i integració del flux de dades de CdC (Recol·lecció, Delegació, etc.) amb la plataforma DEMS.
Fase 4: Auditoria i Serveis d'Auditoria	0.5 Mesos	PC-4: Validació Criptogràfica i Auditoria Funcional	Finalització dels serveis d'auditoria (5.1.5.2, 5.1.5.3) i preparació de la Suite de Tests d'Integració i Robustesa
Fase 5: Validació Final i Desplegament	0.5 Mesos	PC-5: Acceptació Final i Lliurament	Execució de la STIR i acceptació formal per part d'i2CAT (5.3). Lliurament de tot el codi font i documentació final.

6.2. Detall de Terminis d'Execució i Lliurables

La taula següent detalla els lliurables clau que s'han d'entregar i aprovar al final de cada Fase (més enllà dels punts de control formalitzats):

Fita Clau	Termini (Setmana)	Lliurables Associats
PC-1 (Disseny Aprovat)	Setmana 4	D-101 (Especificació Funcional i No Funcional Final), D-103 (Especificació Ontologia Semàntica), D-104 (Pla de Gestió de Claus).
PC-2 (Capa EVM)	Setmana 8	D-102 (Document d'Arquitectura Tècnica), C-201 (Codi Font Contractes Bàsics), Proves de Consens (AC-NF-01 preliminar).
PC-3 (Integració)	Setmana 10	C-202 (Codi Font API RESTful), M-402 (Documentació de l'API), Integració funcional de tots els esdeveniments de CdC.
PC-4 (Auditoria)	Setmana 12	C-203 (Arxius de Desplegament Contenidoritzat), T-302 (Utilitat de Verificació CLI), T-303 (Informes d'Auditoria de Codi Solidity). PC-5 (Acceptació Final)
PC-5 (Acceptació Final)	Setmana 14	T-301 (Resultat Aprovat 100% de la STIR), M-401 (Manual de Manteniment), Lliurament Final de Tot el Codi i Documentació.

6.3. Punts de Control Específics per a la Integració Concurrent

Atès que el mòdul de CdC es desenvolupa concurrentment amb la plataforma DEMS, es defineixen els següents punts d'integració crítica:

- Punt Crític A (Setmana 4): i2CAT ha de garantir que la capa d'autenticació i identitats de la DEMS estigui disponible per permetre la vinculació de les claus públiques dels Agents al registre de CdC (Fase 2).
- Punt Crític B (Setmana 10): L'adjudicatari ha de lliurar a i2CAT les especificacions finals dels punts d'integració per a la càrrega de les dades xifrades de l'evidència (que no es registren a la cadena de blocs, sinó al DEMS) per tal d'implementar correctament les crides de l'esdeveniment de Col·lecció.
- Punt Crític C (Setmana 14): L'adjudicatari ha d'haver adaptat la seva capa de presentació per presentar les sortides JSON-LD de les funcionalitats d'Auditoria (5.1.5.2 i 5.1.5.3) abans de l'execució de la STIR.

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

L'òrgan de contractació ha de designar una persona que assumeixi el control i la coordinació de l'execució contractual amb l'empresa contractista a fi de tractar directament les qüestions relacionades amb el desenvolupament normal de les tasques indicades en aquest plec.

L'empresa contractista ha de designar una persona responsable de la gestió de l'execució del contracte, que haurà de garantir la qualitat de la prestació objecte d'aquest plec, i tractar directament les qüestions relacionades amb el desenvolupament normal de les tasques indicades en aquest plec amb la persona interlocutora designada per l'òrgan de contractació.

Aquestes persones s'han de reunir amb una periodicitat mínima setmanal per tal de supervisar, controlar i tractar qualsevol aspecte vinculat amb el desenvolupament del contracte, a fi d'assegurar que s'està executat de conformitat amb aquest plec.

Per als efectes anteriors, cal avaluar el seguiment i el control del compliment de cada requisit tècnic de la manera següent:

1. Planificació exhaustiva: Elaboració d'una planificació exhaustiva que agrupi les diferents tasques relacionades amb cada requisit, per tal de garantir-ne el compliment.
2. Estat de les tasques: Definició de l'estat de les diferents tasques de desenvolupament, desplegament i integració en quatre categories (*Les tasques poden canviar d'estat d'acord amb les circumstàncies, els acords i les demostracions que es comparteixin durant les reunions de seguiment*):
    a. Planificada
    b. En curs
    c. Pendent de revisió
    d. Acceptada
3. Definició granular de fites relacionades amb la demostració, parcial o total, de la satisfacció dels requisits, sigui de forma individual o conjunta.
4. Acceptació final: Acceptació final d'acord amb els criteris d'acceptació 5.3.

Barcelona, a data de la darrera signatura digital

l'Òrgan de contractació

Sr. Sergi Figuerola Fernández
Director

Sr. Joan Manel Martín Almansa
Director executiu