Generalitat de Catalunya
Centre de Telecomunicacions
i Tecnologies de la Informació

/Salut

LICITACIÓ PER A LA CONSTRUCCIÓ D'UNA PLATAFORMA OBERTA EN SALUT - COMPONENTS D'ARQUITECTURA, MERCAT D'APLICACIONS I SERVEIS DE PLATAFORMA

ANNEX 7: ACCÉS A LES DADES CLÍNIQUES I DEMOGRÀFIQUES

CTTI/2025/113

Barcelona, febrer 2025

Historial de versions i contribucions

Descripció de la revisió	Autor	Datar	Versió
Esborrany inicial		22/01/25	0.1
Revisió		10/02/25	0.3

Índex

1. Introducció

Aquest annex defineix els serveis necessaris per gestionar l'accés a dades clíniques i demogràfiques per part dels diferents components de la plataforma oberta. Els serveis han de garantir la gestió segura, eficient i auditable dels accessos a fonts de dades externes homologades.

El sistema ha de proporcionar:

- Accés controlat a dades en funció del perfil del sol·licitant i del *token* generat per la Plataforma de Seguretat (PDS).
- Creació d'entorns de desenvolupament amb dades anonimitzades i pseudoanonimitzades.
- Gestió de la incorporació de noves fonts homologades a la plataforma per assegurar que es manté la integritat i consistència dels models d'informació origen a les operacions CRUD.
- Control d'execució d'accessos via API Gateway i gestió d'esdeveniments amb els perfils de seguretat acordats.

Les funcionalitats principals inclouen:

- Consulta d'accessos disponibles segons el perfil del sol·licitant.
- Incorporació de nous canals d'accés mitjançant un procés d'homologació.
- Administració del repositori d'accessos i interfícies.
- Control d'ús dels serveis en entorns productius i de desenvolupament.
- Alertes d'intents d'accés no permesos o incorrectes.

El sistema s'ha d'integrar amb els components de seguretat, monitoratge i gestió d'esdeveniments de la plataforma.

2. Requeriments generals d'arquitectura

L'arquitectura del sistema d'accés a dades s'ha de dissenyar considerant les necessitats específiques del sistema sanitari català, caracteritzat per una xarxa complexa d'entitats proveïdores, centres assistencials i professionals distribuïts pel territori. Aquesta arquitectura ha de garantir l'accés eficient i segur a les dades clíniques i demogràfiques, mentre manté els més alts estàndards de privacitat i compliment normatiu.

Un aspecte clau és la gestió segura dels accessos per part d'aplicacions de tercers desenvolupades en el marc de la plataforma oberta. Aquesta capa de seguretat ha de permetre el desenvolupament àgil d'innovacions per part de l'ecosistema, mantenint alhora un control estricte sobre l'accés a dades sensibles. El sistema complementa la seguretat per disseny ja integrada en els models d'informació openEHR, afegint una capa addicional de control i auditoria que se situa entre el repositori de dades clíniques i les aplicacions.

El sistema ha d'implementar una arquitectura distribuïda i resilient, capaç de gestionar grans volums de peticions mentre manté temps de resposta òptims. L'ús de patrons d'arquitectura moderns com microserveis, Event-Driven Architecture (EDA) i cache distribuïda hauria de permetre aconseguir l'escalabilitat i rendiment requerits.+

2.1. Components principals

L'arquitectura s'articula al voltant de tres components principals que treballen de manera coordinada:

1. **Porta d'enllaç d'accés a dades** Component que actua com a punt d'entrada únic per totes les peticions d'accés a dades. Les seves característiques principals són:

    - Validació i autenticació de totes les peticions utilitzant els tokens de la PDS.
    - Implementació de polítiques de control d'accés basades en rols i atributs.
    - Gestió de quotes i límits d'ús per evitar sobrecàrregues.
    - Registre detallat de tots els accessos per auditoria
    - Monitoratge en temps real del rendiment i disponibilitat.
    - Gestió d'errors i excepcions de manera consistent.
    - Implementació de diferencials (patrons *circuit breaker*) per evitar cascades d'errors.

2. **Servei de dades clíniques** Gestiona l'accés al repositori clínic openEHR i altres repositori clínics (p.e.SIMDCAT, genòmica, raw data de dispositius,...) i proporciona:

    - Execució de consultes AQL autoritzades.
    - Validació de permisos d'accés.
    - Registre d'operacions realitzades.
    - Control d'accés a dades restringides.

3. **Servei de dades demogràfiques** Proporciona accés controlat a les dades demogràfiques dels pacients:

    - Consulta de dades al MPI segons permisos.
    - Validació de relacions autoritzades.
    - Registre d'accessos realitzats.
    - Control d'accés segons context.

Així mateix, s'ha d'integrar amb el repositori de recursos de procés de la plataforma i en els seus sistemes i processos d'homologació per la gestió d'accessos i interfícies.

2.2. Mecanismes d'accés

El sistema suporta dos mecanismes d'accés a dades:

1. Via API Gateway

    - Per accessos síncrons.
    - Control d'accés basat en tokens PDS.
    - Auditoria d'operacions.

2. Via gestor d'esdeveniments

    - Per accessos asíncrons.
    - Control d'accés en subscripcions.
    - Auditoria de missatges processats.

3. Requeriments específics

L'ofertant haurà de descriure a la seva oferta, especificant l'aplicabilitat a l'accés a les dades clíniques i demogràfiques com donarà resposta als següents requeriments:

3.1. Requeriments funcionals

3.1.1. Consulta de canals d'accés a dades disponibles

Donar accés a la informació tècnica i funcional dels canals disponibles segons el perfil del sol·licitant que estigui informada al token generat per la PDS.

Disposar de versionat dels mètodes d'us dels canals i la seva situació d'utilització (en producció, nou, obsolet,...) i donar accés a la informació tècnica i funcional corresponent.

3.1.2. Incorporació de nous canals d'accés a dades

Suport a la gestió del procés de sol·licitud, desenvolupament i homologació de nous entorns de desenvolupament. El govern d'aquest procés s'haurà d'integrar amb el procés equivalent d'altres elements de la plataforma.

Aquesta incorporació ha de considerar la homologació en l'us de les integracions a la PDS, monitorització, API Gateway i gestors d'esdeveniments.

3.1.3. Administració del repositori

Identificació de les interfícies API d'administració que ha de proporcionar aquest servei. També es demana un disseny de UI per les funcions d'administració.

3.1.4. Control d'ús

Identificar quins elements fan ús de aquests serveis o tenen previst fer-ho fent control dels entorns productiu i de desenvolupament. Incloure alertes d'intents d'accés no permès o incorrectes addicionalment al que es registri a la monitorització de la plataforma.

3.2. Requeriments tècnics i d'infraestructura

3.2.1. Comuns a la resta de la plataforma.

- Rendiment i escalabilitat i resiliència
- Desplegament en cloud
- Integració amb eines de monitorització i auditoria de la plataforma
- Integració amb PDS
- Integració amb gateway API i gestors d'esdeveniments

3.3. Requeriments d'interoperabilitat amb altres components o sistemes

3.3.1. Seguretat d'accés

El serveis d'accés a dades han de permetre identificar el perfil de seguretat del sol·licitant mitjançant els elements del token de la PDS, assegurar que l'autorització es verificada per els elements que gestionin la integració amb altres sistemes i que en el procés d'homologació del sol·licitant i de la font de dades s'han acordat i implementat els factors de seguretat d'accés i procés.

Es demana la visió lògica de com s'implementarà aquesta seguretat mitjançant la informació de la PDS en el moment de desenvolupament i en el de operació.

3.3.2. Integració amb altres sistemes

Relacionat amb l'apartat anterior aquests serveis han d'interaccionar amb un API Gateway i un gestor d'esdeveniments per aplicar aquesta seguretat a API i a tòpics concrets. Hem de considerar la possibilitat de que es tracti de diversos API GW i/o gestors d'esdeveniments.

Es demana la visió lògica de com s'implementarà aquesta integració i els elements d'arquitectura requerits per la plataforma.