Cerinte tehnice ale Sistemului ECRIS V

Cuprins

Introducere

Proiectul are ca obiectiv principal implementarea unei platforme de gestiune a dosarelor și lucrărilor de la nivelul instanțelor și parchetelor, denumit ECRIS V. Totodata, acest nou sistem IT & C va fi un important instrument în managementul sistemului judiciar, oferind o serie de informații agregate și sistematizate necesare luării unor decizii cu privire la conducerea sistemului judiciar.

Viitorul sistem ECRIS V, ce va fi dezvoltat în cadrul acestui proiect, trebuie sa ofere funcționalități și facilități referitoare la (enumerare ne-exhaustivă):

- Implementarea de noi funcționalități care să acomodeze noile prevederi ale legislației în vigoare;
- interconectarea cu alte sisteme informatice existente, inclusiv implementarea unui standard al datelor;
- fluxurile de documente, inclusiv automatizarea generării de documente sau obținerea lor într-o manieră interactivă;
- pregătirea sistemului pentru utilizarea semnăturii electronice;
- accesare electronică rapidă și sigură a documentelor din dosarele de judecată pentru judecători, procurori, inspectori și consilieri de probațiune, avocați și alte persoane interesate.

ECRIS V va fi construit cu o arhitectură bazată pe servicii (web services) și straturi (layers/tiers), ce va permite ca introducerea de noi funcționalități sau de noi interconectări să se facă cu un minim efort, asigurându-se astfel o bună durată de viață sistemului în condiții corespunzătoare de funcționare.

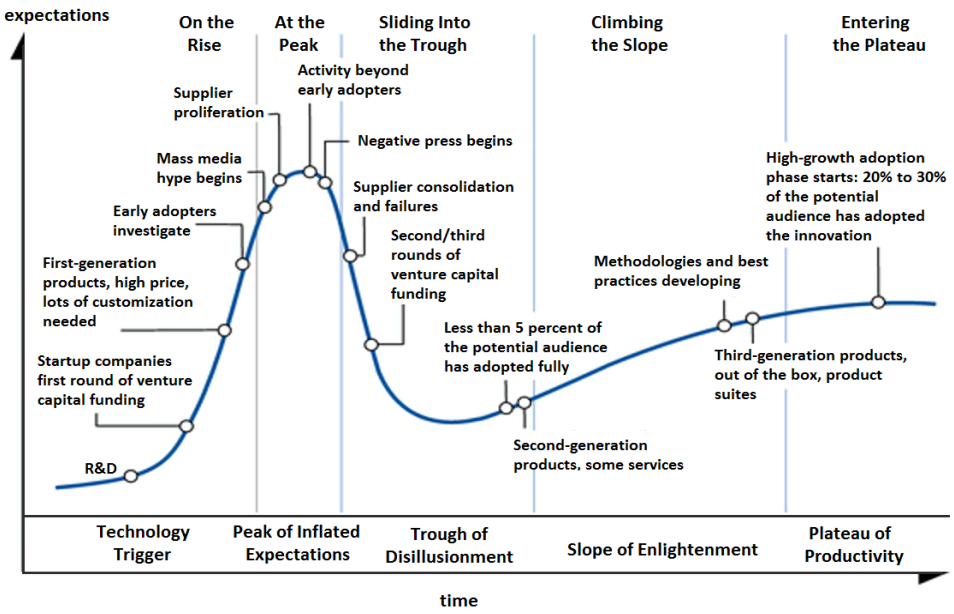
Cerințele sistemului ECRIS V au fost structurate în următoarele componente:

1. Obiective și Principii Generale

Pentru o foarte buna înțelegere a principiilor enunțate mai jos anumiți termeni sunt formulați în mod deliberat în limba engleza, deoarece denumirea în engleză este denumirea universal recunoscută. Traducerea acestor termeni în limba română ar fi deturnat sensul acestora. Un exemplu frecvent este “tenant/tenants” al cărui echivalent în limba română este “locatar/locatari”.

1.1 Tehnologii mature

Pentru implementarea sistemului ECRIS se vor folosi tehnologii testate și mature, precum și abordări tehnice testate și cunoscute. Există o tendință naturală în rândul arhitecților și dezvoltatorilor software de a folosi cât mai curând noi tehnologii înainte ca acestea să ajungă în faza de maturitate (platoul de productivitate din Hype Cycle) ceea ce evident este benefic, însă în același timp crește riscurile tehnice de implementare. Sistemul ECRIS este un sistem de complexitate mare și pentru succesul proiectului este esențială reducerea tuturor riscurilor tehnice. Sistemul ECRIS nu va fi un spațiu de experimente, iar furnizorul va folosi exclusiv tehnologii confirmate și mature aflate în zona “platoului de productivitate”, pentru care există deja atât proiecte de succes implementate, cu o complexitatea similară cu cea a sistemului ECRIS, cât și bune practici documentate.



Figură 1 - Technology Hype Cycle (Sursa: https://en.wikipedia.org/wiki/Hype_cycle)

Compatibilitatea cu versiunile de software de bază
Sistemul trebuie dezvoltat folosind o tehnologie matură, care nu este la prima versiune, compatibilă cu versiunile propuse de sisteme de operare, de platforme de baze de date, pentru care producătorii oferă suport (cele mai recente la momentul punerii în funcțiune).
Tehnologia folosită pentru dezvoltarea sistemului trebuie să fie suportată activ de producător (pentru tehnologiile proprietare) sau comunitare (pentru tehnologiile open-source) și să nu fie o tehnologie aflată la sfârșitul perioadei de utilizare (end-of-life).

1.2 POO – Programare orientată pe obiecte

Sistemul va fi dezvoltat într-un limbaj modern și matur orientat pe obiecte (OOP) de largă utilizare.

1.3 Minimalism și simplitate (KISS - Keep it small and simple)

Ținând cont de complexitatea sistemului ECRIS este important ca furnizorul să evite complexitatea inutilă și să reducă complexitatea componentelor sistemului. “Simplitatea este complexitate rezolvată” (Constantin Brâncuși). Pentru a păstra codul cat mai suplu și pentru a evita complexitatea nenecesară se va evita anticiparea unor modificări înainte ca cerința pentru respectivele modificări să existe.

1.4 Single Responsibility (SOLID)

Fiecare componenta a sistemului (sistem/modul/api/funcție) trebuie proiectată astfel încât să rezolve o problemă cât mai restrânsa și bine definită. În acest fel complexitatea fiecărei componente va fi redusă și sistemul va fi mai ușor extensibil și mentenabil.

1.5 Open-Closed (SOLID)

Extinderea unui comportament este preferabilă în locul modificării. În concret, acest principiu stabilește ca diferitele componente ale sistemului pot fi extinse fără a fi modificat însă comportamentul existent. În termeni POO acest principiu presupune folosirea mecanismelor de moștenire și interfețe pentru a defini comportamentele publice ale claselor care nu vor fi modificate decât prin extindere (moștenire sau implementare). Implementarea este preferabilă moștenirii, deoarece moștenirea creează cuplaje între clase.
Principiul poate fi însă extins și la nivelul altor concepte. Spre exemplu la nivelul API, o metodă API care este deja publicată nu va fi modificată (semnătura sa nu va fi modificată), ci o nouă versiune a metodei va fi publicată. La nivelul bazelor de date, principiul presupune că datele vor fi expuse prin intermediul unor view-uri care ascund detaliile de implementare și persistență. în situația în care structura de persistenta se schimba, view-urile vor rămâne neschimbate în timp ce implementarea poate fi modificată fără a afecta componentele care accesează baza de date.
Extinderea ar presupune doar adăugarea de noi coloane în view-urile existente sau publicarea de noi view-uri. Același principiu se va aplica oricărei componente care ar putea avea dependențe externe.

1.6 Substituție Liskov (SOLID)

Principiul substituției impune ca o clasă care moștenește proprietăți dintr-o clasă de bază să poate fi accesată de apelanți folosind un obiect de tipul clasei de bază. Respectiv o clasă care moștenește o clasă de bază trebuie să respecte regulile logice impuse de clasa de bază.

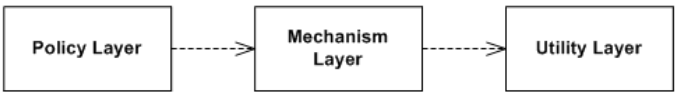
1.7 Segregare interfețe (SOLID)

Principiul se referă la segregarea responsabilității interfețelor în sensul OOP și stabilește ca un apelant al unei componente să nu fie forțat să depindă de componente pe care nu le folosește. În concret interfețele trebuie să fie extrem de bine definite și izolate, astfel încât o clasă care implementează o interfață să nu fie nevoită să implementeze mai mult decât strictul necesar. Principiul ajută la izolarea și restrângerea complexității diferitelor componente și este corelat cu principiul Single Responsability. De asemenea respectarea principiului va reduce gradul de cuplare dintre diferitele componente ale sistemului.

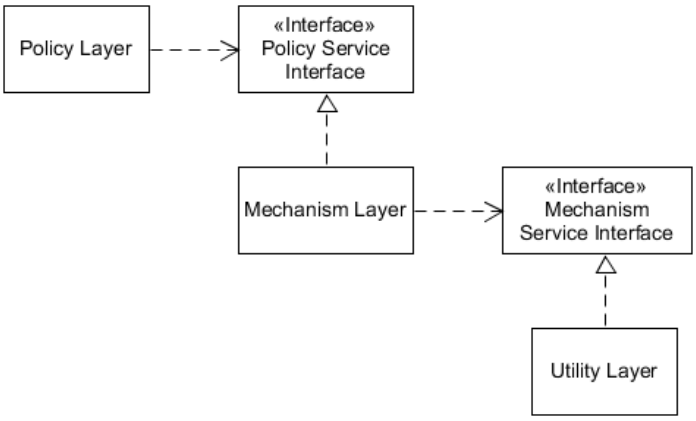
1.8 Dependency Inversion (SOLID)

Într-o arhitectură clasică (spre exemplu o arhitectura 3-layer) care nu aplică principiul inversiunii dependențelor, o componentă de nivel superior (ex: business logic) este direct dependentă de componentele inferioare (ex: data access). Astfel, atunci când o componentă de nivel inferior se modifică este necesară și modificarea componentelor apelante datorită gradului de cuplare dintre acestea. Principiul inversiunii presupune introducerea unui nivel de abstracție între componentele dependente prin folosirea interfețelor (în sensul OOP). În concret, fiind date două componente A și B, unde A depinde de B (A este componenta superioară), principiul impune eliminarea dependenței directe și introducerea interfețelor între cele doua componente pentru a reduce cuplarea, respectiv componenta A va *utiliza* interfețele introduse, în timp ce componenta B va *implementa* interfețele. Astfel ambele componente A și B vor depinde de interfețele introduse care vor avea valoarea unui contract.

Arhitectură clasică



Dependency inversion



Sursa imaginilor: https://en.wikipedia.org/wiki/Dependency_inversion_principle

1.9 DRY (Do not repeat yourself)

DRY este un principiu de bază în dezvoltarea software și presupune eliminarea redundanțelor ce pot apărea în sistemele informatice. Principiul se referă la toate redundanțele ce pot apărea într-un proiect și includ atât redundanțele ce pot apărea în codul sursă, redundanțe ce pot apărea la nivelul datelor, dar și redundanțe la nivelul documentației, testelor șamd.
Furnizorul trebuie să acorde o atenție deosebită în special redundanțelor ce pot apărea la nivelul datelor. Este important ca la proiectarea detaliată, Furnizorul să țină cont de aceste aspecte și să definească foarte clar fluxurile de date între diversele sisteme și componente pentru a evita erorile ce pot apărea. Astfel este important ca în proiectarea bazelor de date să se stabilească o sursă de adevăr pentru fiecare obiect persistat în sistem.

1.10 API First

Toate aplicațiile din sistemul ECRIS vor fi dezvoltate folosind principiul “API First”. Astfel, furnizorul va proiecta în primul rând interfețele programatice ale aplicațiilor (Application Programmatic Interface). Interfețele utilizator (front-end) vor utiliza funcțiile oferite de API și vor fi dezvoltate decuplat (decoupled) de logica de business a API-urilor. API-urile aplicațiilor din sistemul ECRIS vor fi singurul punct de acces la funcționalitatea sistemelor componente.
Acest principiu va asigura o integrabilitate ușoară a aplicațiilor din sistemul ECRIS cu alte aplicații. De asemenea respectarea acestui principiu va asigura un proces de proiectare detaliată mai riguros, cu respectarea principiilor arhitecturale enunțate mai jos și va reduce riscurile tehnice ale proiectului.

1.11 Scalabilitate

Noul sistem trebuie să fie ușor scalabil atât orizontal (prin adăugarea de echipamente hardware suplimentare) cat și vertical (prin creșterea caracteristicilor hardware existente). Relația dintre

performanța sistemului și scalabilitate trebuie sa fie una liniară. Spre exemplu dublarea capacității hardware (orizontal sau vertical) trebuie sa rezulte într-o performanță similară cu dublarea parametrilor de încărcare.

1.12 Performanță

Noul sistem trebuie să fie unul performant. Operațiile uzuale trebuie să poată fi executate imediat și să respecte criteriile de performanță stabilite. Operațiile cu o frecvență mai rară trebuie să poate fi realizate într-un timp rezonabil.

1.13 Flexibilitate și adaptabilitate

Sistemul trebuie să fie flexibil și adaptabil la schimbări atât din punct de vedere al topologiei hardware cât și a arhitecturii software.

1.14 Termeni în limba engleză

În în acest document sunt folosiți în mod deliberat termeni în limba engleză pentru a nu denatura sensul acesta. Un exemplu frecvent este “tenant/tenants” al cărui echivalent în limba română este “locatar/locatari”.

1.15 Tehnologii echivalente

Documentul de arhitectură este un document tehnic cu referințe concrete la anumite tehnologii sau producători de tehnologie. Toate referințele de acest tip trebuie interpretate ca referințe generice care se referă la tehnologia respectivă sau o tehnologie echivalentă, indiferent dacă în textul documentului se folosește sau nu, în mod explicit, sintagma “… sau echivalent”.
Următoarele criterii de succes și obiective trebuie îndeplinite de viitorului sistem ECRIS.

1.16 Ușor de înțeles

Sistemul trebuie să fie ușor de înțeles atât de utilizatorii aplicației, cât și de către echipa tehnică (administratorii, dezvoltatorii software, testeri șamd).
În privința utilizatorilor finali ai aplicațiilor - judecători, procurori, grefieri, registratori, arhivari, avocați, părți etc - este esențial ca sistemul să fie intuitiv și funcțiile frecvente să poată fi folosite cu minim de pregătire. În acest sens sistemul trebuie să respecte regulile de UX specificata în arhitectura UX.
În privința echipei tehnice - administratori, dezvoltatori, testeri - este esențial ca soluția tehnică să respecte regulile și principiile stabilite în documentul de arhitectură și anexele sale, precum și bunele practici de programare.

1.17 Securitate și protecția datelor personale

În mod evident, securitatea informațiilor stocate în sistemul ECRIS este esențială. În acest sens accesul la toate informațiile sistemului trebuie securizat, iar permisiunile vor fi acordate explicit, nu implicit. De asemenea trebuie ținut cont de faptul că anumite informații stocate în sistem trebuie

anonimizate (ex: datele personale ale martorilor protejați, datele personale ale minorilor etc). Noul sistem ECRIS, prin sistemele de portal, va avea o componentă de interacțiune cu publicul. în acest sens este importantă respectarea prevederilor GDPR.
Pentru implementarea securității se va aplica principiul celui mai mic privilegiu (POLP), respectiv unui utilizator sau sistem i se vor acorda doar drepturile strict necesare pentru îndeplinirea unei acțiuni. Mecanismele de securitate vor fi implementate la fiecare nivel al aplicațiilor.
Pentru implementarea mecanismelor de securitate (ex: autentificare) se vor utiliza standarde deschise și componente existente, fiind excluse implementările personalizate (custom).
Flexibilitatea mecanismelor de autorizarea este de asemenea importantă. Pentru a oferi flexibilitatea în privința configurărilor de securitate se va folosi un sistem bazat pe permisiuni tip CBAC (claim based access control) și se va evita folosirea unui sistem tip RBAC (role based access control). Pentru implementarea autorizării se vor folosi componente comune și reutilizabile cu scopul de a crea un sistem foarte robust de definire a drepturilor de acces la resurse (informații, documente, operații etc.). La nivel de baze de date, se vor putea defini permisiuni atât la nivel de coloane (atribute) cat și la nivel de înregistrări (obiecte).

1.18 Trasabilitate

Sistemul trebuie să asigure trasabilitatea completă a tuturor acțiunilor și modificărilor efectuate în cadrul sistemului, inclusiv la nivel de operații de citire. Sistemul trebuie de asemenea să asigure trasabilitatea operațiunilor complexe care pot afecta mai multe înregistrări (spre exemplu: operația de repartizare aleatorie a dosarelor în instanță). În conexiune cu principiile de securitate, sistemul trebuie de asemenea să asigure și trasabilitatea operațiunilor eșuate din lipsa drepturilor de acces care pot indica tentative frauduloase de accesare a unor informații.

1.19 Testabil

Sistemul trebuie să fie unul ușor testabil, în special în mod automat. În acest sens pe parcursul dezvoltării, furnizorul va dezvolta teste automate care vor acoperi cel puțin 80% din funcționalitate și cu prioritate funcționalitățile frecvent utilizate.

1.20 Stabil și predictibil

Sistemul trebuie să fie stabil atât din punct de vedere funcțional (funcționare corectă) cât și al utilizării resurselor hardware, respectiv gradul de utilizare a resurselor hardware trebuie sa fie într-o relație liniară cu încărcarea sistemelor.

1.21 Monitorizabil

Sistemul trebuie să fie ușor monitorizabil. Această caracteristică se referă la capacitatea de a monitoriza ușor următoarele aspecte:

- ✓ utilizarea resurselor de infrastructură (putere de procesare, capacitate de stocare, comunicații șamd);
- ✓ funcționarea corectă a sistemului din punct de vedere tehnic (monitorizarea erorilor, inconsistențelor la nivelul datelor șamd.);
- ✓ buna funcționare din punct de vedere logic prin implementarea de mecanisme auxiliare de verificare a aplicării corecte a anumitor reguli de business importante.

1.22 Extensibil și mentenabil

Noul sistem trebuie sa fie cat mai ușor extensibil. Este de așteptat ca în perioada sa de viață, sistemul să necesite multiple modificări și adaptări ca urmare a modificărilor la nivel legislativ. Arhitectura și designul tehnic trebuie să permită extensibilitatea cât mai ușoară și mentenabilitatea sistemului și a aplicațiilor componente.

1.23 Ușor integrabil

În cadrul sistemului de justiție există foarte multe integrări tehnice necesare între diversele aplicații ale instituțiilor. Aceste integrări fac parte din sistemul ECRIS. De asemenea între instituțiile sistemului de justiție și alte instituții publice sau private există cerințe de integrare. Pentru ca aceste integrări să fie realizabile într-un orizont de timp rezonabil, este absolut necesar ca aplicațiile din sistemul ECRIS să fie ușor integrabile cu alte aplicații.

1.24 Bune practici în dezvoltarea aplicației

Furnizorul trebuie să asigure dezvoltarea codului folosind o metodologie de dezvoltare cunoscută și acceptată de industrie, pusă la dispoziția beneficiarului.
În cadrul dezvoltării aplicației se vor lua în considerare cel puțin:
- Denumire unitară fișiere aferente aplicației
- Denumire unitară și descriptivă a variabilelor folosite
- Organizarea concisă a codului și simplitatea în înțelegere
- Eficiența algoritmilor utilizați
- Fiabilitate și ușurință în menținere / dezvoltare ulterioară
- Mecanisme de testare unitară a codului (unit test)

1.25 Termeni si definiții

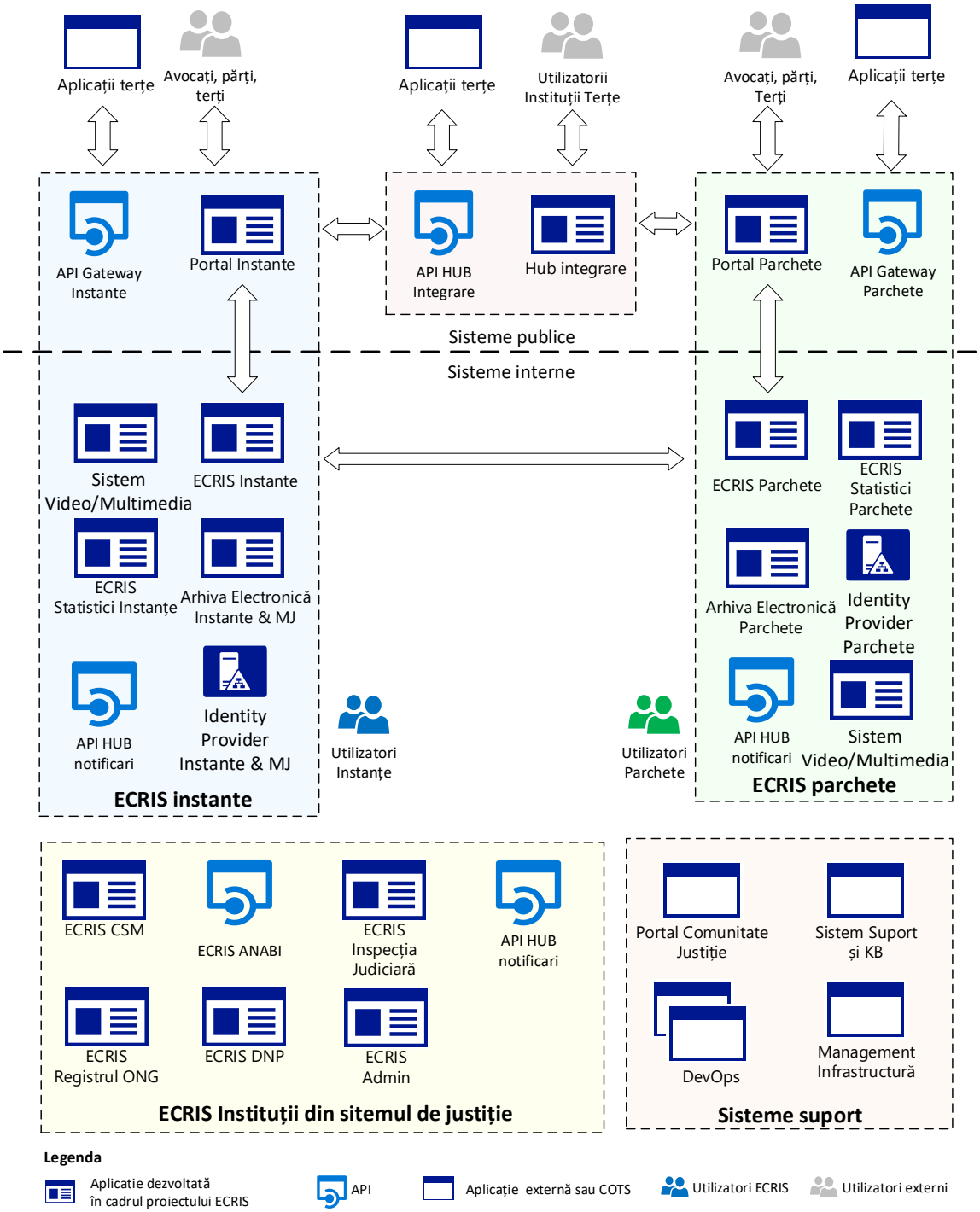
Prezentul document conține o listă a termenilor specifici activității sistemului judiciar. În vederea asigurării unui limbaj comun și evitarea ambiguităților și a înțelegerii diferite care pot apărea între diverse instituții și persoane implicate în proiect, a fost realizat un Glosar de termeni si definiții.
Acest ”Glosar de termeni si definiții” specific sistemului judiciar se regăsește în documentul *„L1.1-Glosar de termeni si definiții”*

2. Arhitectura Conceptuala a Sistemului ECRIS V

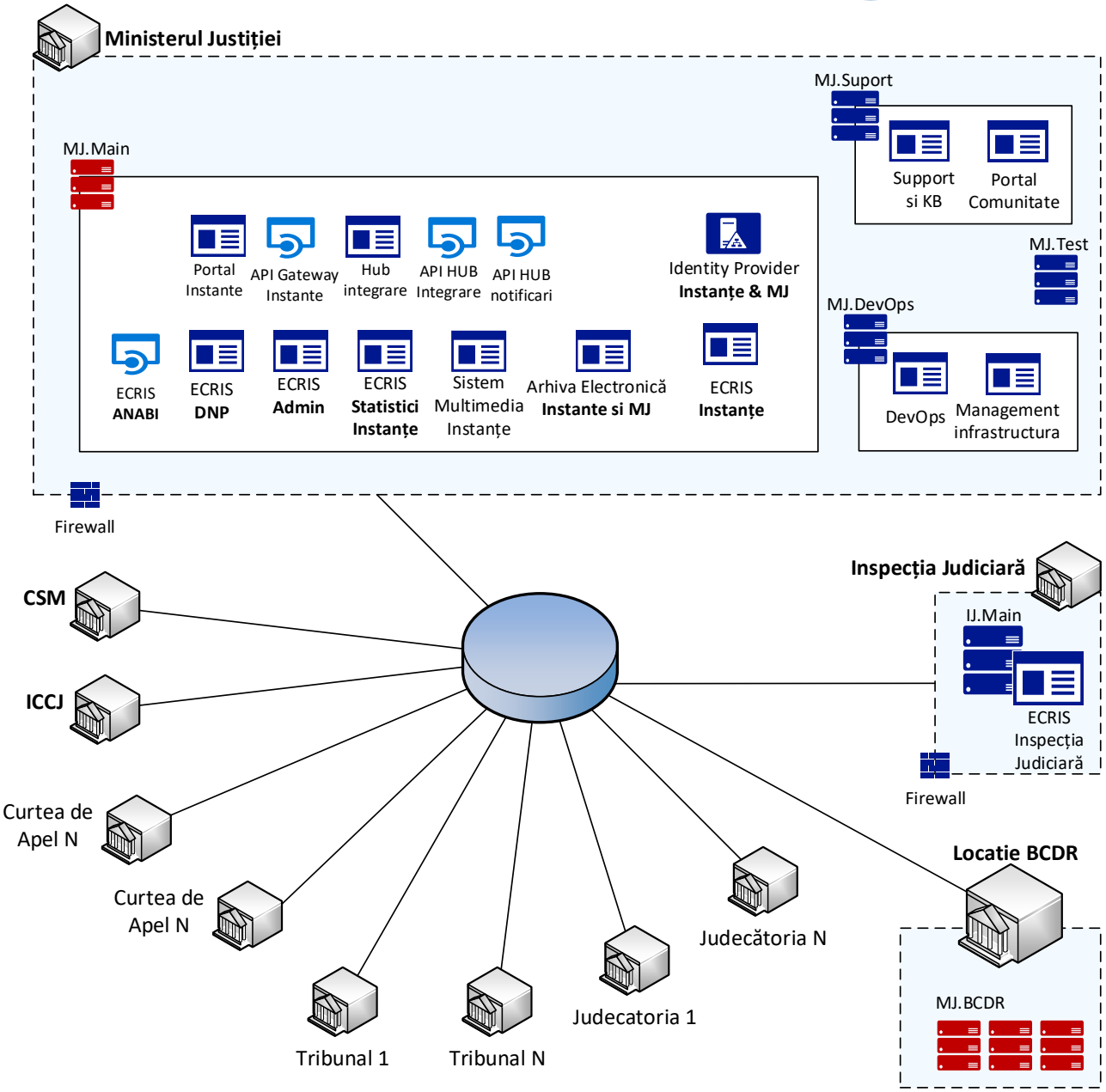
Arhitectura conceptuală prezintă aplicațiile și subsistemele care compun Sistemul ECRIS. Diagramele prezentate mai jos sunt utile pentru a înțelege sistemele și interacțiunile dintre sisteme. Diagramele nu țin cont de aspectele de implementare, respectiv distribuția fizică a sistemelor pe noduri hardware.
Având în vedere modificările semnificative atât la nivel de arhitectură cât și la nivel de funcționalitate, trebuie subliniat faptul că **toate aplicațiile din sistemul ECRIS vor fi dezvoltate pornind de la zero**, fără a refolosi componente sau elemente de logică din versiunea curentă a aplicației.

2.1 Arhitectura Conceptuala conform Analizei Generale

2.1.1 Schema Arhitecturii Conceptuale Generale:

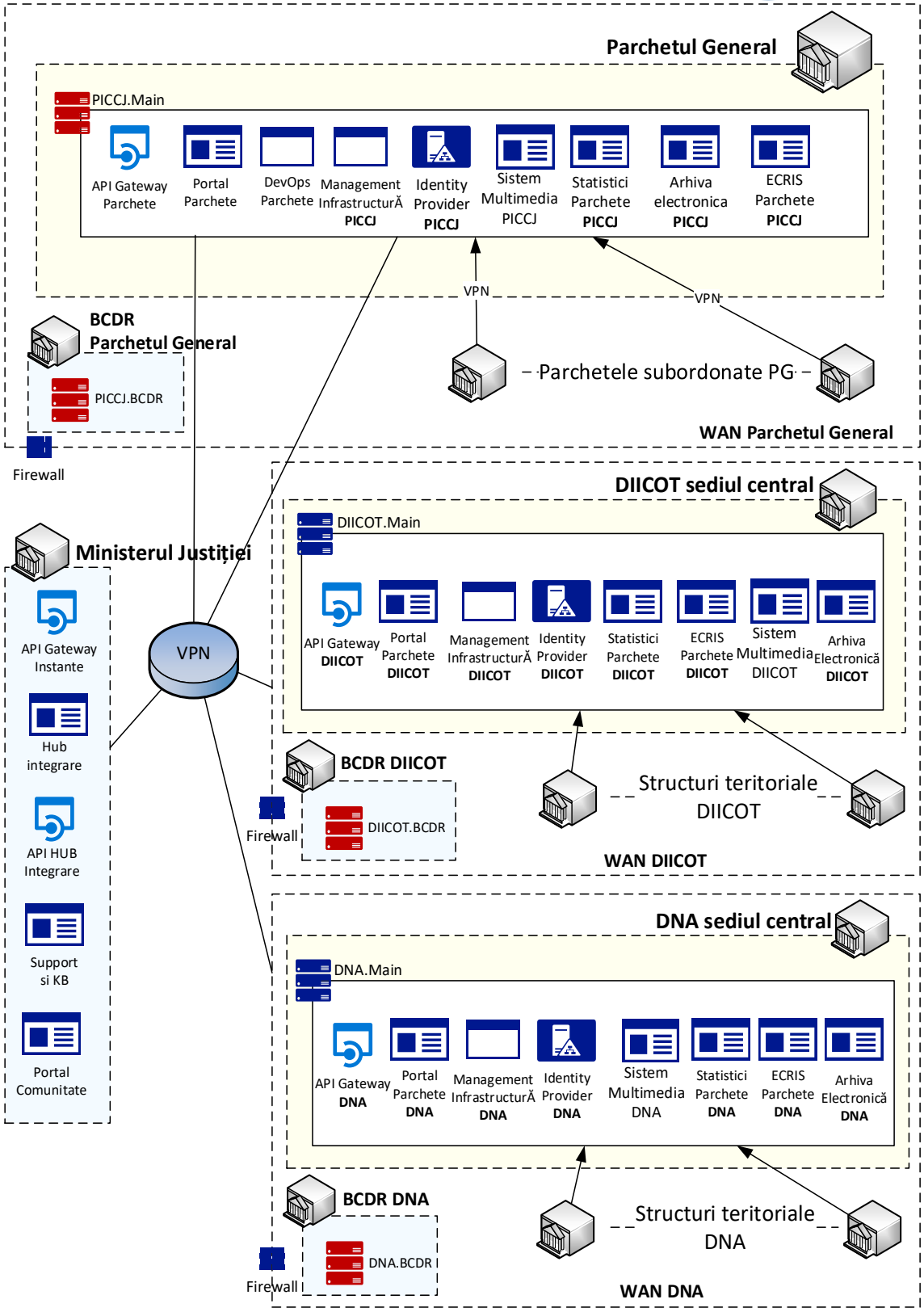


2.1.2 Diagrama de instalare Ecris Instante



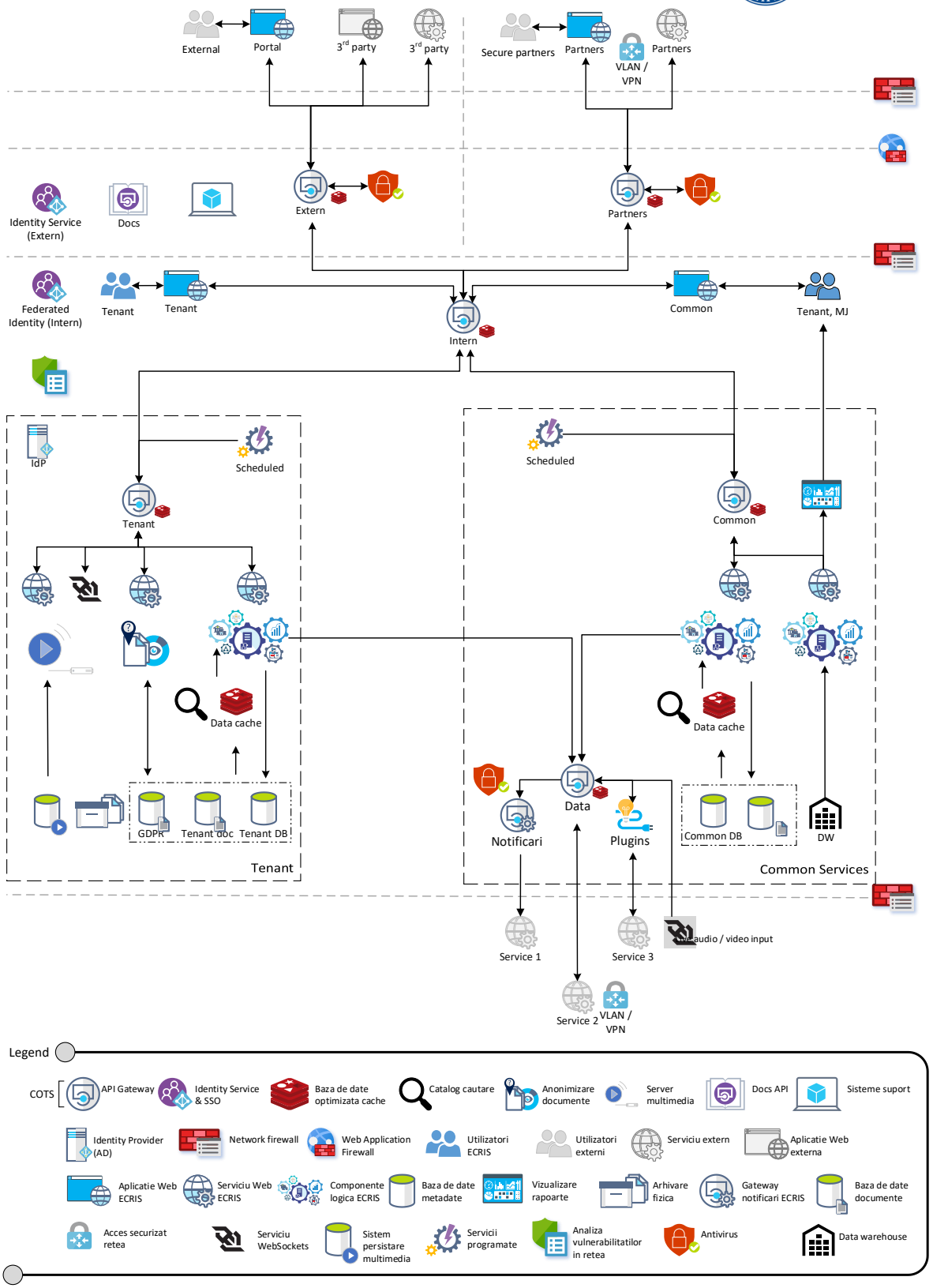
Instalarea aplicației ECRIS Instanțe se va realiza într-o locație pusă la dispoziție de către Ministerului Justiției, aplicație ce va rula pe hardware propriu. Tribunalele, Curțile de Apel, Judecătoriile, CSM și ICCJ vor accesa aplicația pusă la dispoziție de pe aceasta platformă centralizata.

2.1.3 Diagrama de instalare ECRIS Parchete



2.2 Arhitectura tinta conceptuala a Sistemului ECRIS V

2.2.1 Schema Tinta a Arhitecturii Conceptuale Generale



Componente:

2.2.1.1 Public

1. External (users) - utilizatori externi, avocați, cetățeni
2. Portal (App) - aplicații utilizate de utilizatorii externi, parte din ECRIS
3. 3rd Party (App) - aplicații dezvoltate de alte instituții externe pentru conectarea la serviciile publice ECRIS

4. 3rd Party (Serviciu) - serviciu dezvoltat de alte instituții externe pentru conectarea la serviciile publice ECRIS
5. Extern - API Gateway pentru serviciile publice externe
6. Identity Service (Extern) - SSO și identitate pentru utilizatorii externi (external users)
7. Secure partner - utilizatori parte din instituții partenere ce se conecteaza la aplicatie dedicată de integrare ECRIS utilizand o conexiune securizată. Exemplu MAI
8. Partners (App) – aplicație utilizată de utilizatorii ce folosesc conexiune securizată. Exemplu MAI folosind VLAN
9. Partners (Serviciu) - serviciu extern dezvoltat de o instituție partneră ce se conectează la API-ul ECRIS
10. Partners (API Gateway) - API Gateway pentru serviciile expuse instituțiilor partenere
11. Antivirus - componenta ce permite scanarea documentelor incarcate in sistemul ECRIS
12. Sistem suport public - servicii suport incidente, portal comunitate
13. Docs - documentatie API-uri publice

2.2.1.2 Intern

1. Federated Indentity (Intern) - Serviciu de SSO si Federated Identity Management. Această componentă presupune că între beneficiari există o relație de încredere la nivel tehnic
2. Tenant (Users) - utilizatori interni beneficiari: Instante, DNA, DIICOT, PICCJ
3. Tenant (App) - aplicatii dedicate beneficiarilor: Instante, DNA, DIICOT, PICCJ
4. Intern (API Gateway) - API Gateway pentru conectarea la serviciile dedicate per beneficiar sau cele comune
5. Common (App) - aplicatii utilizate de beneficiari, unde cerintele functionale pot fi acomodate pentru toti beneficiarii pe baza de roluri si permisiuni fara a fi necesara dezvoltarea unei aplicatii web dedicate. Exemple: Admin, Arhiva electronica, Statistici, Multimedia, CSM, DNP, JSP
6. Tenant, MJ (Users) - utilizatori interni beneficiari ce acceseaza aplicatiile comune si raportarea complexa/centralizata

2.2.1.3 Intern Tenant

1. IdP - Identity Provider dedicat tenant. Utilizatorul intern se va conecta cu credentialele specifice si va avea acces la datele altor beneficiari tinand cont de permisiunile acordate în baza relației de încredere definită la nivel tehnic între beneficiari
2. Scheduled - Serviciu ce permite declansarea de actiuni recurente / programate sa ruleze la un anumit interval (ex: sincronizari)
3. Tenant (API Gateway) - API gateway pentru conectarea la serviciile dedicate per beneficiar beneficiar
4. Serviciu Web ECRIS - API custom pentru componentele interne
5. Web Sockets API - API ce permite transmiterea prin Web Sockets (scenarii: video / audio on demand folosind serverul de streaming)
6. Server multimedia - Server ce permite redarea materialelor multimedia audio sau video din sistemul de persistare multimedia sau prin conectare la Data API Gateway pentru feed live
7. Sistem persistare multimedia - sistemul unde sunt persistate inregistrarile video / audio
8. Anonimizare documente - serviciu anonimizare documente. Acesta va veni cu o interfata utilizator COTS sau va fi dezvoltata in cadrul ECRIS. Decizia de implementare este in functie de serviciul folosit pentru anonimizarea documentelor

9. Arhiva fizica - componenta pentru arhivarea fizica a dosarelor, dosare arhivate logic in sistemul ECRIS.
10. Grupare conceptuală baze de date - folosită doar pentru simplificarea reprezentării grafice prin care se evidențiază modul de conectare între sursa și destinatie
11. GDPR (baza de date) - baza de date pentru stocarea documentelor anonimizate. Aceasta poate fi separata sau in cadrul Tenant docs, in functie de solutia aleasa pentru anonimizarea documentelor si propunerile de aplicare a securitatii.
12. Tenant doc (baza de date) - baza de date pentru persistarea documentelor asociate la dosare
13. Tenant DB (baza de date) - baza de date pentru persistarea metadatelor
14. Componente logica ECRIS - Fac parte din layer-ul Logic Tier al arhitecturii sistemului ECRIS. Se conecteaza la bazele de date Tenant DB, Tenant Doc, GDPR docs, si la servicii externe prin Data Gateway (descris in Intern Common Services)
15. Data cache - componentă pentru a facilita functionalitățile de căutare avansată și citire dosare. Componenta are rolul de a micșora numărul de cereri de citire din bazele de date. Decizia de implementare a acestei componete vine în urma analizei detaliate ținând cont de cerințele de performanță ale sistemului.
16. Catalog cautare - componentă ce facilitează functionalitatile de cautare simplă și avansată. Componenta are rolul de a micșora numărul de cereri de citire din bazele de date. Decizia de implementare a acestei componente vine în urma analizei detaliate ținând cont de cerințele de performanță ale sistemului. Căutările se vor face folosind componenta de Data cache.

2.2.1.4 Intern Common Services

1. Scheduled - Serviciu ce permite declanșarea de acțiuni recurente / programate să ruleze la un anumit interval (ex: sincronizari)
2. Common (API Gateway) - API gateway pentru conectarea la serviciile reutilizate de toți beneficiarii.
3. Serviciu Web ECRIS - API custom pentru componentele interne.
4. Componente logica ECRIS - Fac parte din layer-ul Logic Tier al arhitecturii sistemului ECRIS. Se conecteaza la bazele de date Common DB, Common Doc, si la servicii externe prin Data Gateway.
5. Data cache - componentă pentru a facilita funcționalitățile de căutare avansată și citire metadate și documente. Componenta are rolul de a micșora numărul de cereri de citire din bazele de date. Decizia de implementare a acestei componente vine în urma analizei detaliate ținând cont de cerințele de performanță ale sistemului.
6. Catalog cautare - componentă ce facilitează funcționalitățile de căutare simplă și avansată. Componenta are rolul de a micșora numărul de cereri de citire din bazele de date. Decizia de implementare a acestei componente vine în urma analizei detaliate ținând cont de cerințele de performanță ale sistemului. Căutările se vor face folosind componenta de Data cache.
7. Data (API Gateway) - Reprezinta componenta prin intermediul căreia sunt asigurate serviciile de interfațare cu alte sisteme externe (Remote services). Prin aceasta componentă se pot împinge ("Push") datele din ECRIS către sistemele externe - scriere în sisteme externe, se pot trage ("Pull") datele din sisteme externe - citire din sisteme externe.
8. Notificări (API Custom) - serviciu web ce are rolul de a trimite mesajele primite de la beneficiar către serviciul corespunzator ținând cont de cerințele tipului de mesaj (Email, SMS) și cerințele de conectare la serviciul extern (server SMTP, API server email, API server SMS).

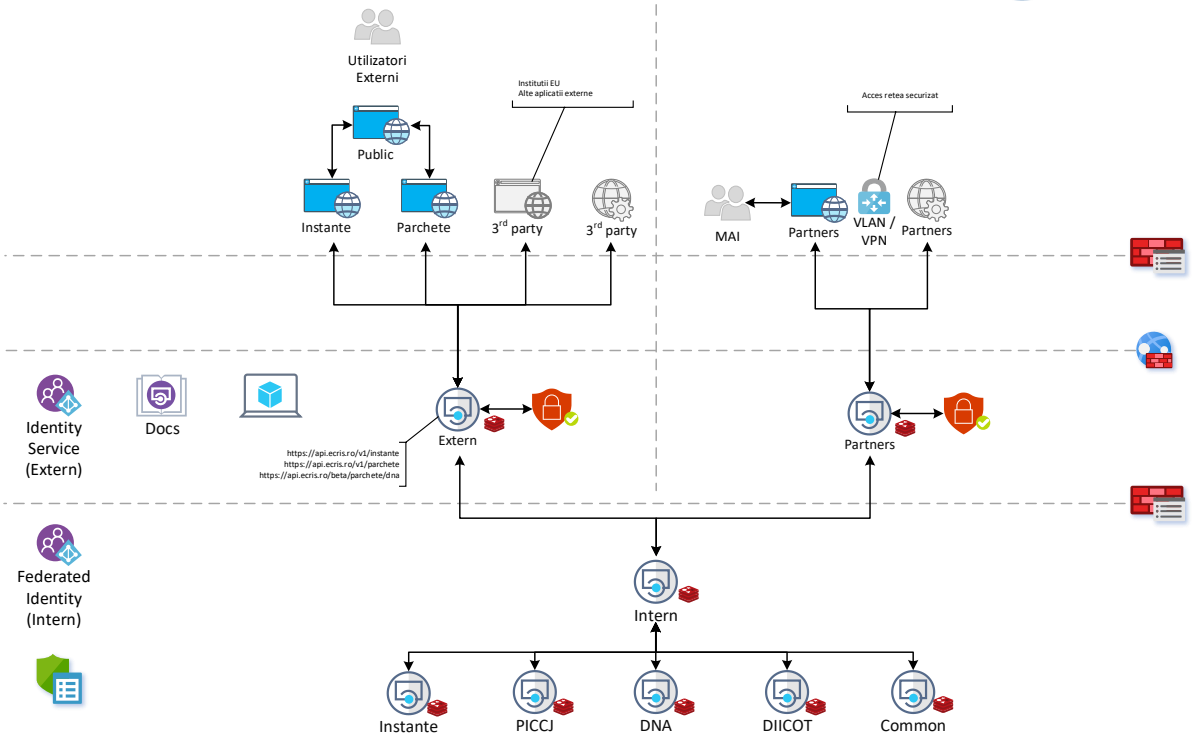
9. Plugins (Connector) - posibilitatea de a configura un conector la nivel de API Gateway pentru integrările complexe unde nu se justifică (performanță, scalabilitate, securitate, reutilizare) construirea unui API Custom.
10. Conectare utilizand o conexiune securizata VPN - posibilitatea de conectare la un serviciu extern folosind IP Whitelisting, conexiune VPN sau alte cerințe de securitate suplimentară pentru conectarea la servicii externe. Aceasta capabilitate va fi detaliată în urma analizei detaliate pentru integrarile cu serviciile externe atunci cand sistemul ECRIS scrie sau citeste informatii din alt sistem.
11. DW - componentă pentru centralizarea datelor primare și statisticile din cele 4 sistem operaționale, cros sistem judiciar.

- Datele sunt centralizate pentru toti beneficiarii la nivel de tranzactie operationala, analizate si agregate.
- Datele reprezintă date primare folosite in mod uzual, prelucrate în prealabil în vederea eliminării informațiilor de identificare personală
- Centralizarea datelor se face cu o frecvență predefinită.
- Datele vor fi versionate istoric. Astfel, un raport generat la închiderea unei luni, anterioare momentului analizării (ex. luna noiembrie reprezinta momentul analizei, iar luna octombrie este luna analizată), pe langă datele introduse în cursul lunii analizate, ar trebui să conțină și date din perioada următoare (în cazul exemplului dat, luna noiembrie - momentul analizei), pentru a fi evidențiate și eventualele modificări / corecții efectuate ulterior lunii analizate.

12. Rapoarte și statistică (vizualizare și logică) - componentă de tip COTS ce permite construirea de rapoarte complexe.
    - ✓ Rapoartele și statisticile ce afișează ultima modificare din sistem (în timp real) vor fi accesate din aplicatiile Web cu sursa de date direct din Tenant DB folosind ECRIS UI Framework, componenta DataGrid.
13. Common DB - baza de date pentru metadate comune. Poate fi folosită de exemplu pentru nomenclatoarele comune. Se va detalia in analiza detaliată.

Common Docs - baza de date persistentă cu documente comune. Se va detalia in etapa de analiză detaliată a proiectului.

2.2.2 Schema Tinta a Arhitecturii Conceptuale pentru Acces Public si Access Securizat Utilizatori Externi



Componente

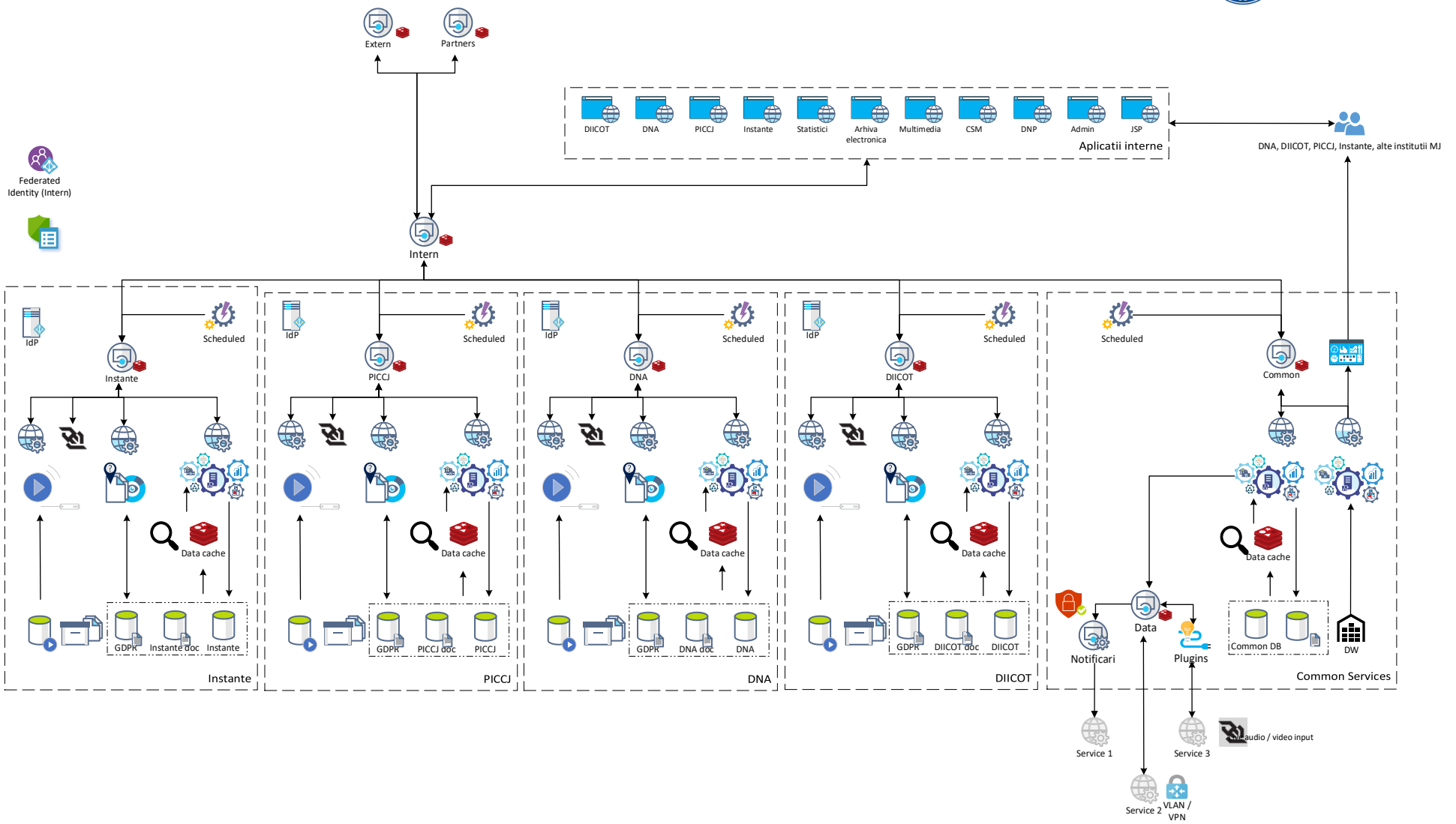
2.2.2.1 Public

1. External (users) - utilizatori externi, avocați, cetățeni
2. Public (App) - aplicație ce utilizează aplicațiile publice de instante și parchete
3. 3rd Party (App) - aplicații dezvoltate de alte instituții externe pentru conectarea la serviciile publice ECRIS
4. 3rd Party (Serviciu) - serviciu dezvoltat de alte instituții externe pentru conectarea la serviciile publice ECRIS
5. Extern - API Gateway pentru serviciile publice externe
6. Identity Service (Extern) - SSO și identitate pentru utilizatorii externi (external users)
7. MAI - utilizatori parte din MAI (instituție parteneră) ce se conectează la aplicația dedicată de integrare ECRIS utilizând o conexiune securizată.
8. Partners (App) - aplicație utilizată de utilizatorii ce folosesc conexiune securizată. Exemplu MAI folosind VLAN.
9. Partners (Serviciu) - serviciu extern dezvoltat de o instituție parteneră ce se conectează la API-ul ECRIS.
10. Partners (API Gateway) - API Gateway pentru serviciile expuse instituțiilor partenere.
11. Antivirus - componentă ce permite scanarea documentelor încărcate în sistemul ECRIS.
12. Sistem suport public - servicii suport incidente, portal comunitate
13. Docs - documentație API-uri publice.

2.2.2.2 Intern

1. Federated Indentity (Intern) - Serviciu de SSO și Federated Identity Management. Această componentă presupune că între beneficiari exită o relație de încredere la nivel tehnic.
2. Intern (API Gateway) - API Gateway pentru conectarea la serviciile dedicate per beneficiar sau cele comune.
3. Instante API Gateway - API Gateway dedicat pentru Instante
4. PICCJ API Gateway - API Gateway dedicat pentru PICCJ
5. DNA API Gateway - API Gateway dedicat pentru DNA
6. DIICOT API Gateway - API Gateway dedicat pentru DIICOT
7. Common API Gateway - API Gateway dedicat pentru serviciile comune

2.2.3 Schema Tinta a Arhitecturii Conceptuale pentru Access Utilizatori Interni



Nota: Componentele au fost definite la punctele anterioare.

3. Arhitectura Software ECRIS V

3.1 Arhitectura logică generală aplicații ECRIS

În *figura de mai jos* este ilustrată arhitectura general aplicabilă tuturor aplicațiilor din sistemul ECRIS. În mod evident această arhitectura va fi declinată în funcție de specificul fiecărei aplicații.
Arhitectura urmează un model N-Tier, astfel fiecare aplicație va fi structurată în trei niveluri (tiers):

- **Nivelul de prezentare (UI Tier)**
  Va asigura interfața sistemului cu utilizatorii prin intermediul interfeței utilizatori și interfața cu sistemele externe prin intermediul API.
- **Nivelul de logică (Application Tier)**
  Va asigura implementarea logicii fiecărei aplicații.
- **Nivelul de date (Data Tier)**
  Va asigura persistența meta datelor, persistența documentelor și indexarea informațiilor în scopul căutării rapide.

Arhitectura permite ca fiecare nivel să fie distribuit pe mai multe noduri, în scopul scalării orizontale. Spre exemplu, într-un scenariu de mare încărcare (cum sunt portalul Instanțelor, portalul PICCJ) nivelul de prezentare poate fi distribuit balansat pe mai multe servere. În mod similar nivelul de logică poate fi distribuit pe mai multe servere, în timp ce nivelul de date poate de asemenea fi distribuit pe mai multe partiții orizontale (shard-uri) ce pot fi distribuite pe mai multe servere.
Pentru claritate, trebuie evidențiată distincția între termenii în limba engleză „Tier„ și ”Layer”, al căror echivalent apropiat în limba română este “Nivel”, respectiv diferența dintre arhitectura N-Tier și N-Layer.
Segmentarea de mai sus se referă la termenul englezesc de Tiers, în sensul unei arhitecturi N-Tier, respectiv la separarea fizică a componentelor de sistem, componente ce au o reprezentare distinctă și pot fi distribuite pe mai multe servere (e.g. aplicații distincte).
Din punct de vedere al limbajului de programare este recomandată implementarea aplicațiilor din sistemul ECRIS folosind un limbaj de programare de nivel înalt OOP (Object-oriented programming), type safety (mecanism de prevenire a erorilor în limbajele de programare), de largă utilizare. Toate aplicațiile din sistemul ECRIS vor fi implementate folosind același set de tehnologii.
Tehnologii candidat

- **Limbaj de programare:** .Net C#, Java sau echivalent

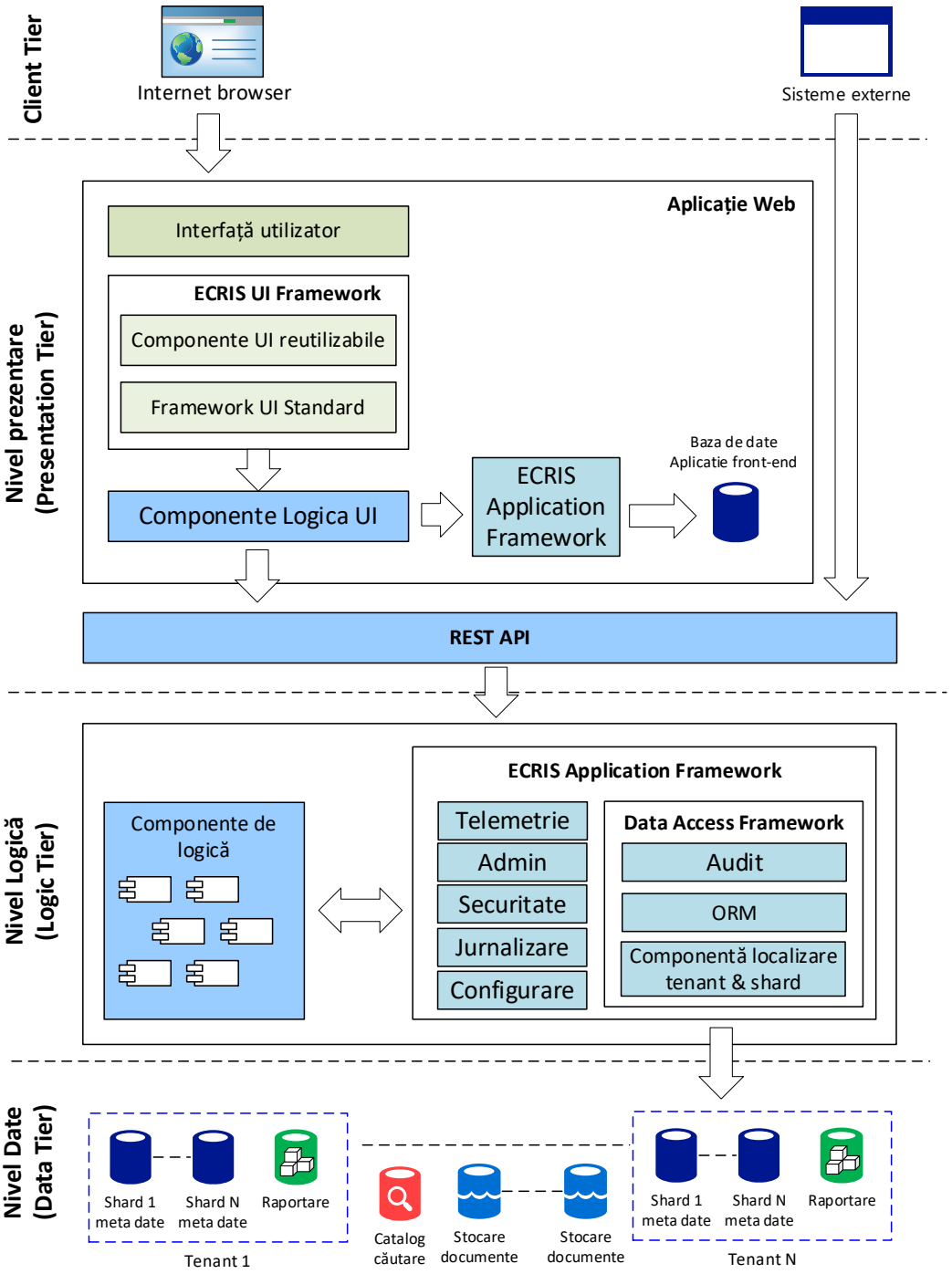


Figure 1 - Arhitectura logică a aplicațiilor din sistemul ECRIS

3.2 Nivelul de prezentare (Presentation Tier)

3.2.1 Interfața utilizator

Interfața utilizator va fi implementată ca o aplicație web distincta de tip SPA (Single Page Application) care va apela API-ul. La nivelul interfeței utilizator NU se va implementa logică de aplicație (business logic).

La nivelul interfeței utilizator se poate implementa strict logica tipică de UI (afișare și introducere), logică de navigare UI, logică de validare, logică de asistență a utilizatorului șamd. Validarea va fi integral implementată la nivel de aplicație (API), dar fiecare aplicație ar putea implementa suplimentar validări preventive pentru evitarea apelurilor inutile către API și pentru a îmbunătăți ergonomia interfeței.
Toate aplicațiile web (front-end) din sistemul ECRIS vor fi dezvoltate folosind un set comun de componente și servicii UI reutilizabile ce vor fi oferite de ***ECRIS UI Framework*** (descris mai jos).
Toate interfețele utilizator din sistemul ECRIS vor respecta arhitectura și regulile UX definite în documentul ECRIS L2.3.B – Arhitectura UI-UX.
Aplicația web poate dispune și de o bază de date locală pentru a persista diferitele informații ce țin strict de logica de interfață utilizator, spre exemplu preferințele utilizatorilor, însă în această bază de date nu se vor stoca informații de business, spre exemplu informații despre dosare. Eventual această bază de date poate persista referințe spre obiectele logice de business (ID-uri). Persistarea informațiilor de business în această bază de date în scop de caching ar trebui evitată pentru a evita complicarea inutilă a logicii aplicației front-end și pentru a evita inconsistențele la nivel de date.
Pentru accesul la baza de date, servicii legate de securitate, jurnalizare și audit, aplicația web va utiliza serviciile comune oferite de ***ECRIS Application Framework*** (descris mai jos).
Toate aplicațiile din sistemul ECRIS trebuie să permită personalizarea interfeței de către utilizator, aceasta fiind una din limitările versiunii actuale care provoacă nemulțumiri în rândul utilizatorilor. În acest sens interfețele utilizator trebuie să permită diverse operații de personalizare, printre care:

- Configurarea meniurilor.
- Configurarea temei de culori (se vor oferi cel puțin doua teme: pe fond alb și pe fond întunecat).
- Configurarea paginii principale de start.
- Configurarea filtrărilor, sortărilor, a dimensiunii coloanelor și posibilitatea salvării setărilor
- Salvarea de referințe către diverse informații din sistem (tip favourites).
- Configurarea notificărilor și a modalităților de primire a notificărilor.
- Etc.

3.2.2 Pentru utilizatorii externi

Prezentarea topografiei de navigație către informațiile disponibile utilizatorilor externi, prin intermediul Nivelului de Prezentare(Cadru Interfață Utilizatori).

- Ghidul și instrucțiunile de utilizare a portalului
- Informații despre dosare și ședințe
- Informații de baza (de nivel înalt) despre arhitectura ECRIS
- Informații juridice diverse
- Atlas judiciar
- Informații referitoare la modalitățile de acces și manipulare a datelor cu caracter personal din dosarele accesibile
- Întrebări generale frecvente și răspunsurile aferente
- Cadrul de introducere de documente în format electronic
- Diferite funcționalități de configurări personalizate (meniuri, culori, filtre, notificări, etc)
- Link-urile de acces către sub-portalurile de Instanțe, Tribunale și Curți de Apel, ICCJ (micro-site-uri web cu informații specifice fiecărei instanțe în parte – similar cu ce se regăsește acum pe portal.just.ro pentru fiecare instanță).

Utilizatorii externi autentificați (conform mecanismelor specifice de autentificare) vor avea acces la mai multe informații, conform cu rolul de acces configurat. Mai multe detalii despre tipurile de

utilizatori externi, modalități de autentificare și roluri asociate se regăsesc în **Livrabilul L2-Portal Instanțe-Specificații funcționale.pdf**

3.2.3 Pentru Utilizatorii Interni

- Toate funcționalitățile disponibile utilizatorilor externi, incluzând accesul la sub-portalurile de Instanțe (micro-site-uri web cu informații specifice fiecărei instanțe în parte – similar cu ce se regăsește acum pe portal.just.ro pentru fiecare instanță).
- Ghidul de utilizare al funcționalităților specifice utilizatorilor interni (din sistemul judiciar) care au drepturile necesare
- Funcționalitățile specifice utilizatorilor din sistemul judiciar
- Implementează logica funcționalităților de Frontend care include și conectivitatea cu nivelul arhitectural următor (REST API)
- Funcționalitățile UI specifice administrației ECRIS
- Funcționalitățile UI specifice pentru depanare și diagnostic folosite de echipele DevOps și Test

3.3 API (Application Programming Interface)

3.3.1 Concepte generale privind API

Din punct de vedere conceptual componenta API este situată în cadrul nivelului de prezentare. Cu toate acestea din punct de vedere al împachetării (packing) aceasta va fi cuplată cu nivelul de logică. **Componenta API va fi implementată folosind o arhitectură de tip REST și formatare JSON. API-ul va implementa un standard REST, spre exemplu OData (recomandat), ORDS sau echivalent.**
Componenta API a oricărei aplicații va fi documentată folosind un standard de documentare tip Swagger sau echivalent. Documentația API va fi publicată online, iar accesul la documentație va fi eventual restricționat în funcție de cerințele fiecărei instituții. Este recomandat ca documentația API să fie disponibilă public, indiferent de restricțiile aplicate pentru accesul la API. În acest fel se vor facilita integrările cu diversele aplicații externe.

IMPORTANT: la nivel european există inițiativa European Interoperability Framework de definire a unor standarde de interoperabilitate pentru sistemele administrației publice. O componentă importantă a EIF este ISA2 (https://ec.europa.eu/isa2/isa2_en) – "Interoperability solutions for public administrations, businesses and citizens". Dezvoltarea API-urilor ECRIS trebuie să fie aliniată cu eforturile europene de interoperabilitate și standardizare. În acest sens în faza inițială a proiectului de implementare se va evalua progresul ISA2 și/sau alte inițiative de standardizare la nivel european. La momentul elaborării documentului de arhitectura ISA2 definește câteva soluții reutilizabile. Dintre acestea, soluția de Core Vocabularies (vocabular comun) definește câteva scheme reutilizabile de entități, cum ar fi Persoană, Agent, Adresă, Organizație publică, Document etc. Desigur aceste concepte nu acoperă necesitățile ECRIS, totuși pot fi aplicate în modelarea domeniului pentru ECRIS V, astfel încât alinierea la un standard european comun de interoperabilitate să poată fi realizată mai ușor.

Tehnologii candidat

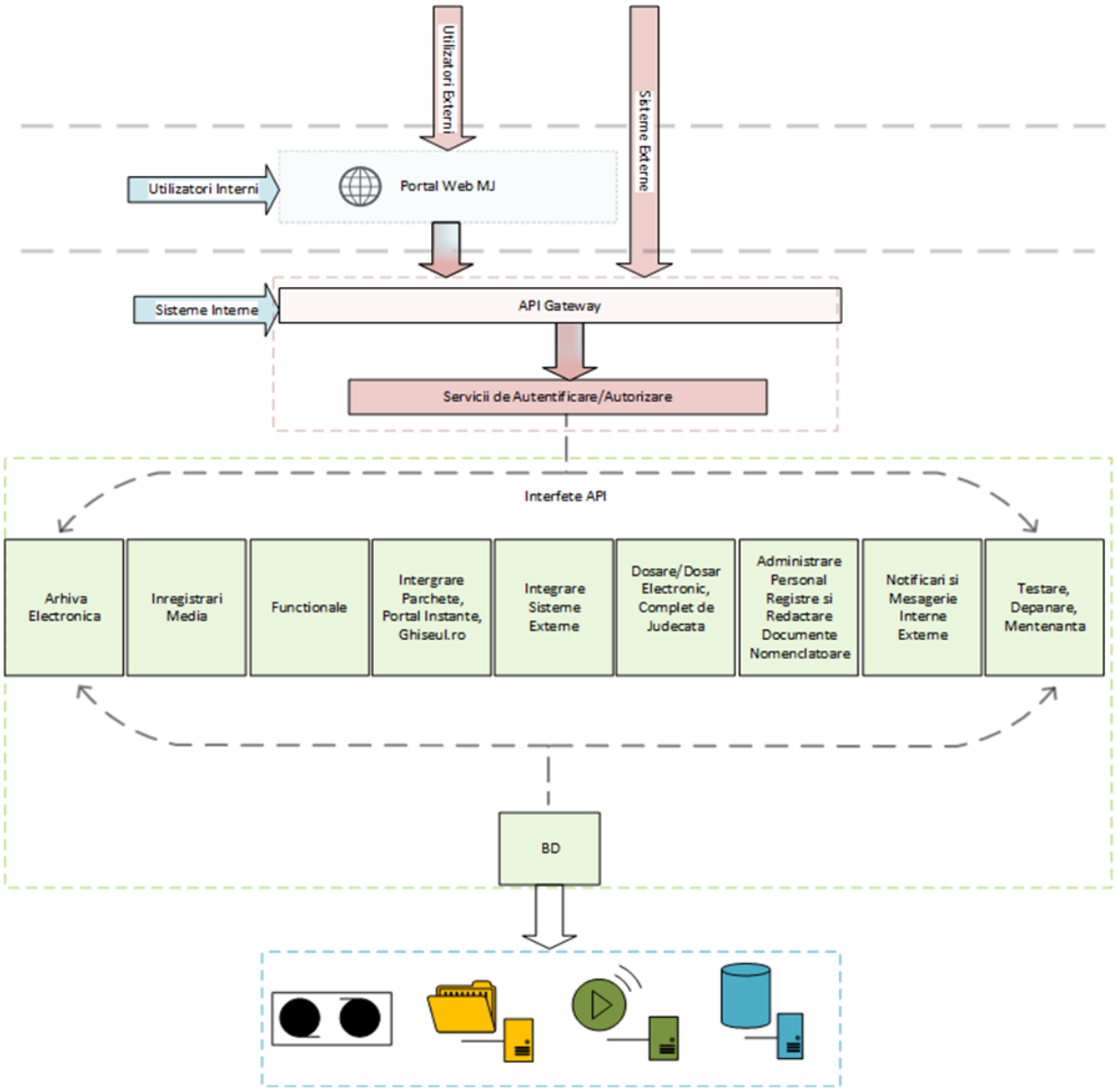
- **Standard API**: OData, ORDS sau echivalent + ISA2 sau versiuni viitoare

Documentare API: Swagger sau echivalent

3.3.2 Componentele Principale ale API

Nivelul acesta joacă rol de interfața de legătura și control între nivelul Prezentare (Interfețe utilizator), nivelul Logic-Tier (funcționalitățile) și bazele de date ECRIS. La acest nivel se definesc

API-urile de acces în sistem, validarea sau invalidarea utilizatorilor și implementează unul din nivelele de securitate ale sistemului (API Gateway). Aici sunt validați atât utilizatorii ce ajung prin intermediul portalului de mai sus cât și utilizatorii automați (alte sisteme) atât din exterior (cum ar fi de exemplu integrarea cu Politia de Frontieră) cât și cei considerați ca fiind parte din sistemul ECRIS însă sunt externi implementării particulare MJ sau Parchete.



Componentele acestui nivel sunt următoarele:

- API validare și conectare utilizatori interni
- API validare și conectare utilizatori externi
- API validare și conectare sisteme interne
- API validare și conectare sisteme externe
- API de legătură cu funcționalitățile de logică ECRIS
- API Arhiva Electronică
- API Înregistrări Media
- API Integrare Parchete, Portal Instanțe, Ghișeul.ro (Interne)
- API Integrare Sisteme Externe

- API Dosare și Complet Judecată
- API Administrare Personal, Registre, Redactare Documente și Nomenclatoare
- API Notificări și Mesagerie Diversă
- API de Testare, Depanare, Mentenanță
- API BD

3.4 Nivelul de logică (Logic Tier)

Nivelul de logică va implementa logica efectivă a aplicației. Logica va fi separată în componente de logică bine definite, conform principiului de responsabilitate unică (Single Responsibility). Fiecare componentă va oferi servicii (metode) ce ulterior vor fi împachetate (wrapped) ca servicii ale API.

IMPORTANT: comunicarea dintre tenants în cadrul aceluiași nod se poate realiza direct, evitând un apel la API, ceea ce ar putea aduce îmbunătățiri de performanță. Pentru ca această comunicare ”in-process” să fie posibilă, fără apariția de erori, este necesar ca metodele API să împacheteze strict metodele publice ale componentelor de logică, fără să implementeze logică suplimentară. În caz contrar apare riscul semnificativ al apariției unor erori foarte greu de depistat.

3.4.1 Componentele Principale ale Nivelului de Logica

Acest nivel poate fi considerat ca fiind motorul aplicației ECRIS Instanțe. Aici va fi implementată marea majoritate a componentelor de business ECRIS. Funcționalitățile vor fi împărțite în blocuri. Aceste blocuri vor fi protejate la accesul oricărui utilizator, în funcție de permisiunile acestuia. Detalierea tuturor funcționalităților din acest nivel (la fel ca și ale celorlalte nivele) vor fi prezentate în capitolele următoare. Acest nivel are acces la nivelul de permanența a datelor.

• Protecția este implementata prin nivelul superior de securitate care va avea, printre alte funcții de protecție ECRIS, și sarcina de selecție a funcționalităților ECRIS per utilizator. Acest bloc de securitate este cel care comunica direct cu nivelele superioare prezentate anterior. Aici toți utilizatorii vor fi validați, în funcție de permisiunile și drepturile de acces la date și funcționalitățile pe care le dețin, fie ca este vorba de utilizatori umani fie de sisteme. Tot la acest nivel se va realiza înregistrarea de utilizatori noi.

• Blocul de logica de audit și telemetrie. Aceste doua funcționalități sunt menite sa înregistreze toate acțiunile pe care utilizatorii sau sistemele le vor efectua asupra sistemului ECRIS. Aceste funcționalități vor oferi posibilitatea auditării oricărui eveniment, acțiune, precum și a utilizatorilor care le-au efectuat pe de o parte, pe de altă parte, aceste informații înregistrate vor folosi la diagnostic și investigații despre funcționarea sistemului, informații ce sunt necesare echipelor de DevOps, Test și eventual Suport.

• Blocul de Configurări folosește la: configurații interne ale sistemului ce sunt menite sa asigure funcționarea optima a acestuia.

• Blocul de funcționalități de business se va găsi tot la acest nivel. Acesta la rândul lui va fi împărțit în sub-componente de funcționalități astfel încât securitatea și protecția la acces și utilizare a fiecărei funcționalități va fi posibilă. Ca funcționalități de bază menționăm adăugarea de noi documente, citirea documentelor existente, gestionarea dosarelor și a documentelor cuprinse în acestea, funcționalitățile de notificări, toate funcționalitățile relative integrării cu sisteme interne și externe. O parte din funcțiile logice de administrație de sistem și depanare vor fi integrate tot în acest nivel

3.4.2 Nivelul de persistență a datelor (Data Tier)

La acest nivel se asigură persistența datelor stocate de aplicație. Acestea pot fi împărțite conceptual în două categorii de informații primare: metadate (înregistrările efective din bazele de date) și documente. În categoria acestor documente intră documente electronice scanate, documente electronice generate de aplicații, documente externe, fișiere video sau audio etc.

Notă: În 0 Arhitectura logică generală aplicații ECRIS, pictogramele sunt folosite în scop strict ilustrativ pentru a evidenția capabilitatea multishard a arhitecturii. Concret, atât baza de date de documente cât și catalogul de căutare ar putea fi distribuite pe mai multe partiții orizontale.

3.4.2.1 Persistarea metadatelor

Metadatele aplicației vor fi ținute într-o bază de date relațională ce va utiliza o arhitectură modernă optimizată pentru bazele de date relaţionale, arhitectură care să conţină toate componentele necesare (servere pentru gestionarea şi procesarea bazelor de date, soluţie de stocare a datelor, infrastructură de comunicaţii), capabile să asigure disponibilitate, performanţă ridicată, scalabilitate, dar şi administrarea şi gestionarea centralizată de multiple baze de date. Soluţia optimizată pentru bazele de date relaţionale reprezintă nucleul care asigură consolidarea şi centralizarea bazelor de date replicate şi care va trebui să fie capabil să susţină baze de date relaţionale de ordinul zecilor de TB, redundante şi robuste, să asigure prevenirea întreruperilor în funcţionare şi un timp minim de recuperare în caz de erori hardware, software şi umane.
Tehnologia de baze de date trebuie să fie una matură pentru care există un istoric de proiecte de succes de complexitate similară sistemului ECRIS. De asemenea tehnologia de baze de date trebuie să fie una larg utilizată în România, astfel încât să se evite o relație de dependență față de furnizor.

IMPORTANT: consistența și integritatea relațională a datelor din sistemul ECRIS este critică, astfel sistemul de baze de date folosit trebuie să asigure integritate relațională și tranzacții cu proprietăți ACID (Atomic, Consistent, Izolat, Durabil). Din acest motiv NU sunt acceptabile soluții tehnice de persistare a metadatelor care nu respectă aceste condiții. În concret, nu sunt acceptabile sisteme de baze de date non-relaționale (NoSQL).
Pentru aplicațiile care vor stoca un volum mare de date (în special ECRIS Instanțe, ECRIS Parchete, Portal Instanțelor și Portal Parchete) metadatele vor fi partiționate orizontal (sharding). Strategia de sharding va fi analizată în faza de analiză detaliată. În aplicațiile sistemului ECRIS care stochează volume mari de informație, informațiile sunt în general grupate în jurul conceptelor de dosare (Instanțe și parchete) și lucrare (parchete). Această structură a informațiilor favorizează partiționarea datelor. O strategie potențială este partiționarea în shard-uri care vor acoperi o anumită perioadă calendaristică în ani sau în shard-uri care să țină cont de indicatorul de arhivare logică.
IMPORTANT: în cazul aplicațiilor unde volumul de date este redus se recomandă evitarea partiționării pentru a reduce complexitatea aplicației.

3.4.3 Cerinţe generale pentru soluţia de sistem de gestiune baze de date

Sistemul de gestiune al bazelor de date relaţionale din cadrul soluției trebuie să fie disponibil comercial (COTS – Commercial off the Shelf) și să poată rula pe sistemul de operare ofertat și să aiba suport asigurat de catre producator. Pentru a răspunde cerinţelor de funcţionalitate şi performantă, sistemul de gestiune a bazelor de date relaţionale trebuie să prezinte următoarele capabilităţi minime şi obligatorii:

1. Serverul de baza de date trebuie să permită folosirea a peste 48GB memorie

2. va permite folosirea a minim 24 de nuclee de procesare (core-uri fizice procesor) pentru procesările de tip SQL pentru fiecare instanță;
3. va asigura nivelurile de izolare ANSI SQL și va oferi suport pentru funcționalitățile de bază pentru limbajul SQL
4. va putea interoga direct din baza de date fișiere text externe, fără a necesita în prealabil o operațiune de încărcare a acestora într-o tabelă dedicată precum și posibilitatea de a rula automat anumite scripturi la momentul interogării acestor fișiere externe;
5. va permite reorganizarea, mutarea și redefinirea de fișiere de date, tabele și indecși fără blocarea activității utilizatorilor la datele aflate în curs de modificare, indiferent de dimensiunea acestora;
6. va oferi diferite metode de indexare a datelor;
7. sa permită paralelizarea operațiilor de tip DML si DDL (insert, update, delete, merge, create, interogări, etc) pentru o reducere semnificativa a timpului necesar efectuării acestor operații;
8. va permite ajustarea dinamica și automată de către baza de date a parametrilor de memorie astfel încât zonele de memorie să fie dimensionate în concordanță cu tipul de operații ce se desfășoară la un moment dat;
9. va permite compresia datelor din tabele;
10. să aibă mecanisme built-in de replicare a datelor;
11. să posede mecanisme de partiționare a tabelelor;
12. să suporte built-in tipuri de date in format XML/JSON.
13. Instrumente de dezvoltare a obiectelor din baza de date: soluția trebuie să ofere unelte de dezvoltare pentru modulele ETL (Extract, Transform, Load), pentru design-ul bazelor de date atât relaționale cât și multidimensionale, pentru design-ul rapoartelor.
14. Criptarea transparentă a datelor, a fișierelor de date și a fișierelor jurnal fără să fie necesară modificarea aplicației.
15. auditarea trebuie să includă informații despre momentul în care au fost citite datele, în plus față de orice modificare a datelor.
16. Produsul trebuie să ofere caracteristici precum configurarea îmbunătățită și managementul auditurilor.
17. Produsul să definească specificațiile de audit în fiecare bază de date, astfel încât configurația auditului să poată fi adaptată pentru diversele bazele de date.
18. Posibilitatea de a filtra evenimentele auditate; posibilitatea de a customiza operația de audit în funcție de evenimentele din baza de date.
19. facilități de optimizare și depanare a performanței server-ului de baze de date, pentru a furniza administratorilor o perspectivă interactivă cu privire la performanță.
20. Sistem de monitorizare extins al evenimentelor: sistem general de tratare a evenimentelor la nivel de server prin captarea, filtrarea și reglarea evenimentelor generate de procesele de server. Evenimentele trebuie să poată fi captate și exportate în diferite formate de ieșire, inclusiv în formatul utilizat de sistemul de operare gazdă, pentru corelarea cu aplicațiile sistemului de operare și ale bazelor de date, permițând astfel o monitorizare completă a sistemului.
21. Comprimarea backup-urilor
22. Sistemul trebuie sa permită implementarea administrării bazate pe politici pentru:
    a. Definirea și managementul politicilor de configurare a sistemului;
    b. Monitorizarea și prevenirea modificărilor asupra sistemului prin crearea de politici dedicate;
    c. Detectarea problemelor de conformitate cu politicile, direct din interfața de administrare a server-ului;

d. Posibilități de virtualizare;
e. Soluția SGBD oferită să ofere posibilitatea instalării, fără costuri adiționale, a unui număr nelimitat de baze de date distincte în mașini virtuale alocate serverului licențiat.

Soluția trebuie sa nu impună nicio restricție din punct de vedere licențiere aferentă numărului de utilizatori ce se pot conecta la SGBD.

3.4.4 Arhivarea logică

În cadrul sistemului ECRIS vor fi prevăzute două tipuri de arhivare: logică și permanentă. Arhivarea logică va păstra informațiile în sistemele de stocare online iar informațiile arhivate vor fi marcate logic ca fiind arhivate (flag de arhivare). Arhivarea permanentă va presupune transferarea efectivă a datelor în sisteme de arhivare dedicate cu caracteristici WORM.

IMPORTANT: pentru arhivarea logică datele vor fi păstrate în aceleași tabele și baze de date, dar vor fi marcate logic ca fiind arhivate, respectiv datele NU vor fi transferate în alte tabele sau baze de date dedicate arhivei logice. Transferul datelor arhivate logic în cadrul aceleiași baze de date generează în timp complexitate nenecesară care nu poate fi ușor controlată și din acest motiv, această abordare NU este recomandată. Această abordare a fost folosită în ECRIS 4 și versiunile anterioare unde și-a dovedit ineficacitatea. Astfel datele arhivate logic vor fi păstrate în aceleași tabele cu datele nearhivate, iar filtrarea se va realiza prin intermediul unor structuri de tip view (recomandat) sau la nivel de logică de aplicație. Pentru aplicațiile care folosesc sharding, este recomandat ca datele arhivate să fie persistate în shard-uri dedicate arhivei logice pentru a descărca bazele de date online, cu condiția ca distribuirea să facă parte din strategia normală de sharding. Altfel spus este esențial ca datele arhivate logic să NU primească un tratament separat în logica aplicației (în afara eventualei filtrări logice), respectiv o interogare (query) care cuprinde atât date nearhivate cât și date arhivate logic nu trebuie să fie cu nimic diferită față de o interogare care cuprinde doar date nearhivate sau doar date arhivate. În eventualitatea în care datele arhivate sunt stocate în shard-uri separate, un astfel de query va fi rezolvat prin mecanismul general de interogare multi-shard, în mod transparent pentru componentele de logică ale aplicației.

3.4.5 Persistarea (stocarea) documentelor

Spre deosebire de metadate, documentele NU vor fi stocate într-o baza de date relațională. Pentru stocarea documentelor este recomandată fie stocarea documentelor pe sistemul de fișiere folosind o tehnologie integrată cu baza de date (Microsoft SQL Server FILESTREAM, Oracle BFILE sau echivalent) fie folosirea unei baze de date orientate pe documente/NoSQL (MongoDB+GridFS, HDFS, CouchDB sau echivalent).
La nivelul documentelor, operațiunile permise vor fi de adăugare, ștergere și adăugare versiune. Astfel conținutul unui fișier încărcat nu va putea fi modificat decât prin adăugarea unei versiuni în situațiile în care logica aplicației permite acest comportament.
IMPORTANT: Așa cum se observă în diagramă (0 Arhitectura logică generală aplicații ECRIS), bazele de date de documente nu aparțin unui tenant. Acest detaliu va permite referențierea unui document în cadrul aceluiași nod de către tenants diferiți, respectiv documentele vor fi partajate intre tenants la nivel tehnic. În cazul nodurilor multi-tenant, respectiv nodurile care găzduiesc datele mai multor instituții, cum este cazul nodului centralizat MJ sau în cazul celor trei instalări centralizate din cadrul parchetelor (PICCJ, DNA și DIICOT), există oportunitatea păstrării unei referințe unice la un document

atunci când un document este folosit în mai multe dosare, fără ca acesta să fie duplicat. Acest caz este foarte comun în cazul căilor de atac când dosarul este transferat pentru apel/recurs la instanța superioară. La transferul dosarului toate documentele dosarului trebuie să ajungă și la instanța superioară. Întrucât ambele Instanțe sunt găzduite pe același nod, duplicarea documentelor nu este necesară. Acest comportament este posibil având în vedere că documentele nu se vor modifica, ci doar se vor versiona. Astfel referențierea versiunilor unui document este posibilă. Comportamentul de referențiere este esențial din motive de economie de spațiu.

3.4.6 Raportare

Pentru raportare se vor folosi baze de date distincte, astfel încât interogările de raportare să nu afecteze performanța aplicațiilor principale. În funcțiile de cerințele de raportare ale aplicației, bazele de raportare pot fi replici OLTP peste care opțional se pot construi baze de date OLAP. Implementarea de baze de date OLAP este recomandată cel puțin pentru aplicațiile de Statistici, Statistici ECRIS Instanțe și Statistici ECRIS Parchete.

3.4.7 Catalog căutare

Pentru funcțiile de căutare se va folosi o tehnologie de indexare (Elastic Search, Apache Solr sau echivalent). Opțional și aceasta poate fi partajată între tenants.
Tehnologii candidat:

- **Sistemul de baze de date**: Microsoft SQL Server, Oracle Database sau echivalent
- **Stocare documente**: Microsoft SQL Server FILESTREAM, Oracle BFILEs sau echivalent. Alternativ MongoDB+GridFS, HDFS, CouchDB sau echivalent.
- **Sharding**: Elastic Data Client Library, Oracle RAC sau echivalent
- **Indexare și căutare**: Elastic Search, Apache SolR sau echivalent.

Tehnologiile Software ce vor fi folosite pentru realizarea aplicației ECRIS sunt următoarele:
Software de bază:

- **Sistem de operare**: Windows Server 2019+ sau echivalent (cea mai recentă versiune disponibilă comercial de la producător).
- **Sistem baze de date**: SQL Server 2019+, Oracle Database 19c+ sau echivalent (cea mai recentă versiune disponibilă comercial de la producător)
- **Web server**: Internet Information Services (IIS) sau echivalent (cea mai recentă versiune disponibilă comercial de la producător)
- **Virtualizare: Hyper-V, VMWare sau echivalent** (cea mai recentă versiune disponibilă comercial de la producător)
- **Arhivare: Veeam sau echivalent** (cea mai recentă versiune disponibilă comercial de la producător)

Tehnologii de dezvoltare:

- **Limbaj de programare: .Net C#, Java sau echivalent**
- **ORM**:Entity Framework Core, NHybernate, Hybernate sau echivalent
- **Standard API: OData, ORDS sau echivalent + ISA2 recomandat**
- **Documentație API: Swagger sau echivalent**
- **Framework UI: React, Angular sau echivalent**
- **Javascript typesafe: TypeScript, Flow sau echivalent**
- **Componente UI: Kendo UI, componente opensource sau echivalent**

Bazele de date

- **Storage documente: FILESTREAM, BFILE, MongoDB, CouchDB, HDFS sau echivalent**
- **Catalogare/indexare: Elastic Search, Apache SolR sau echivalent**
- **Sharding: Elastic Data Client Library, Oracle RAC sau echivalent**

4. ECRIS Instante si ECRIS Parchete

ECRIS Instante si ECRIS Parchete reprezinta componentele principale („core") ale viitorului sistem ECRIS V. Toate celelalte componente ale sistemului sau al proiectului ECRIS V reprezintă componente suport sau adiacente acestor componente principale. De aceea este foarte important ca ofertantul sa analizeze cu responsabilitate cerintele funcționale ale acestor componente astfel încat estimarea efortului privind implementarea acestora sa fie una cat mai realista.

4.1 ECRIS Application FRAMEWORK

Componenta ECRIS Application Framework va asigura serviciile și comportamentele comune nivelului de logică. Utilizarea acestei componente comune va asigura reducerea efortului de dezvoltare și reducerea defectelor.
Pentru accesul la date se va folosi o platformă de tip ORM . În cadrul sistemului ECRIS jurnalizarea informațiilor este esențială, astfel ECRIS Application Framework va asigura tuturor aplicațiilor, funcțiile necesare pentru auditarea evenimentelor. Rolul componentei de Audit în zona de Data Access este acela de a asigura că accesul la informațiile din bazele de date este auditat (inclusiv operațiile de citire), pentru prevenirea erorilor și omisiunilor în timpul dezvoltării (situația în care dezvoltatorii omit să auditeze o operație).
Dincolo de auditarea tehnică a operațiilor la nivelul bazelor de date este necesar ca înregistrările de audit să aibă și o semnificație în contextul unei operații logice (semantică), respectiv este necesar ca semnificația fiecărei operații să fie implementată în cadrul componentelor logice. În acest sens este recomandată folosirea unui instrument de analiză statică a codului (Roslyn, Resharper sau echivalent) care va genera erori blocante în cazul în care operații expuse public nu conțin și codul aferent de audit.
În cazul distribuirii informațiilor pe mai multe shard-uri, pentru identificarea shard-ului în care se află un anumit obiect, la nivel de Data Access se va folosi o componentă pentru localizarea shard-ului în care obiectul se află.
IMPORTANT: serviciul de localizare a unei partiții/shard este prezentat conceptual în documentul de arhitectură, însă în faza de design detaliat, este obligatorie utilizarea unor tehnologii existente și/sau facilități oferite de sistemul de baze de date pentru implementarea partiționării (Elastic Database Client Library, Oracle Sharding/RAC sau echivalent). NU este recomandată implementarea logicii de sharding la nivelul aplicației.
Componenta va mai oferi de asemenea servicii pentru implementarea uniformă a autorizării și a configurărilor.
Funcțiile acestei componente definite la nivel de arhitectură nu sunt exhaustive și vor fi extinse în faza de proiectare detaliată a sistemului.
Tehnologii candidat

- **ORM**: Entity Framework, NHybernate, Hybernate sau echivalent
- **Sharding**: Elastic Database Client Library, Oracle RAC sau echivalent

4.2 ECRIS UI FRAMEWORK

În privința utilizatorilor finali ai aplicațiilor - judecători, procurori, grefieri, registratori, arhivari, avocați, părți etc - este esențial ca sistemul să fie intuitiv și funcțiile frecvente să poată fi folosite cu minim de pregătire. În acest sens sistemul trebuie să respecte regulile de UX specificate în arhitectura UX.
Interfața utilizator va fi implementată ca o aplicație web distincta de tip SPA (Single Page Application) care va apela API-ul. La nivelul interfeței utilizator NU se va implementa logică de aplicație (business logic).
La nivelul interfeței utilizator se poate implementa strict logica tipică de UI (afișare și introducere), logică de navigare UI, logică de validare, logică de asistență a utilizatorului șamd. Validarea va fi integral implementată la nivelul de aplicație (API), dar fiecare aplicație ar putea implementa suplimentar validări preventive pentru evitarea apelurilor inutile către API și pentru a îmbunătăți ergonomia interfeței.
Toate aplicațiile web (front-end) din sistemul ECRIS vor fi dezvoltate folosind un set comun de componente și servicii UI reutilizabile ce vor fi oferite de ***ECRIS UI Framework*** (descris mai jos).
Toate interfețele utilizator din sistemul ECRIS vor respecta arhitectura și regulile UX definite în documentul ECRIS L2.3.B – Arhitectura UI-UX.
Aplicația web poate dispune și de o bază de date locală pentru a persista diferitele informații ce țin strict de logica de interfață utilizator, spre exemplu preferințele utilizatorilor, însă în această bază de date nu se vor stoca informații de business, spre exemplu informații despre dosare. Eventual această bază de date poate persista referințe spre obiectele logice de business (ID-uri). Persistarea informațiilor de business în această bază de date în scop de caching ar trebui evitată pentru a evita complicarea inutilă a logicii aplicației front-end și pentru a evita inconsistențele la nivel de date.
Pentru accesul la baza de date, servicii legate de securitate, jurnalizare și audit, aplicația web va utiliza serviciile comune oferite de **ECRIS Application Framework** (descris mai jos).
Toate aplicațiile din sistemul ECRIS trebuie să permită personalizarea interfeței de către utilizator, aceasta fiind una din limitările versiunii actuale care provoacă nemulțumiri în rândul utilizatorilor. În acest sens interfețele utilizator trebuie să permită diverse operații de personalizare, printre care:

- Configurarea meniurilor prin salvarea unei liste de opțiuni favorite
- Configurarea temei de culori (se vor oferi cel puțin doua teme: pe fond alb și pe fond întunecat)
- Configurarea paginii principale de start
- Configurarea filtrărilor, sortărilor, a dimensiunii coloanelor și posibilitatea salvării setărilor
- Salvarea de referințe către diverse informații din sistem (tip favourites)
- Configurarea notificărilor și a modalităților de primire a notificărilor
- Etc

ECRIS UI Framework este o platformă comună (framework) care va fi utilizată de toate aplicațiile sistemului ECRIS pentru implementarea interfețelor utilizator. Această platformă va îngloba toate componentele și serviciile comune necesare pentru implementarea interfețelor utilizator și va asigura un tratament unitar al interfeței utilizator, precum și respectarea regulilor definite în arhitectura UI/UX. Dezvoltarea acestei platforme va reduce considerabil costul dezvoltării, prin evitarea duplicării în cadrul diferitelor aplicații și de asemenea va reduce numărul de defecte. Scopul acestei componente este să reducă semnificativ efortul de dezvoltare al interfețelor utilizator.
ECRIS UI Framework va fi dezvoltată având la bază o platformă client-side de largă utilizare (React, Angular sau echivalent).
Platforma va conține diverse componente comune de UI reutilizabile (DataGrid, Editor de texte, meniuri, tab controls, sliders, dialog etc.). Componentele platformei vor fi dezvoltate folosind una sau mai multe librării existente de componente (Kendo UI, Angular Material, Material-UI sau alte

librării echivalente). O atenție deosebită trebuie acordată componentei DataGrid, respectiv componenta care va afișa informații în format tabelar. Această componentă trebuie să ofere diverse comportamente configurabile, avansate, precum:
- Selecție multipla de înregistrări
- Filtrarea înregistrărilor
- Sortarea înregistrărilor, inclusiv multipla
- Paginare, inclusiv prin scroll virtualizat (încărcare dinamica la scroll)
- Editare în row (editarea unei înregistrări direct în tabel)
- Gruparea înregistrărilor
- Export în excel
- Redimensionarea vizuală a coloanelor
- Agregări (totaluri, subtotaluri)
- Vizualizări tip master-detail / părinte-copil (afișarea a doua tabele relaționate one-many)
- Reordonare înregistrări
- etc.

Platforma va asigura de asemenea diverse servicii și comportamente comune, cum ar fi:
- personalizarea interfeței utilizator și persistarea preferințelor utilizator, spre exemplu salvarea configurărilor meniurilor făcute de fiecare utilizator;
- logică de navigare ierarhică în cadrul aplicațiilor (meniuri, submeniuri, breadcrumbs etc.)
- comportament comun pentru validare și afișarea mesajelor de validare și a erorilor
- comportament comun pentru afișarea erorilor

Pentru codul JavaScript se va folosi o componentă care să asigure “type safety” (TypeScript, Flow sau echivalent).
Pentru codul de stilizare CSS se va folosi o componentă care asigură un comportament dinamic stilurilor (less sau echivalent).
Este de asemenea recomandată folosirea unei componente care să minimizeze codul JavaScript și CSS (Minify sau echivalent).
IMPORTANT: În cazul folosirii unor componente terțe (third-party) furnizorul trebuie să se asigure că licența componentei este compatibilă cu sistemul ECRIS. Proprietatea intelectuală asupra codului sursă va fi deținută de Ministerul Justiției, iar codul sursă al aplicațiilor nu va fi făcut public. Astfel, în cazul folosirii de componente open source se vor folosi doar componente cu licențiere tip BSD sau echivalent (BSD, MIT). Nu se vor folosi licențe tip GNU GPL, inclusiv LGPL sau orice altă licență care obligă la publicarea codului sursă derivat în domeniul public. În cazul componentelor comerciale se vor folosi doar licențe tip “Royalty free”, de asemenea Furnizorul va asigura licențierea componentelor comerciale inclusiv pentru personalul beneficiarului, astfel pentru fiecare componenta comercială se vor asigura 10 licențe de dezvoltare. Nu se vor utiliza componente comerciale care presupun licențe cu cost variabil în funcție de numărul de proiecte, site-uri, volum de utilizare, limitate în timp sau orice altă variabilă, decât cu acordul formal al beneficiarului.
Tehnologii candidat
• Framework UI: React, AngularJS sau echivalent
• JavaScript typesafe: TypeScript, Flow sau echivalent
• Componente reutilizabile: Kendo UI sau echivalent

Pentru a asigura consistență din punct de vedere UI/UX și o experiență cât mai cursivă și productivă pentru utilizatori, vor trebui respectate principile de design enuntate in documentul Anexa 2 - L2.3.B-Arhitectura UI-UX.docx.

In cadrul anexei L2.3-Exemple UI-UX-1.0.pdf beneficiarul pune la dispozitia ofertantului si un exemplu de funcționalități solicitate pentru aceasta componentă.

4.3 ECRIS Instante

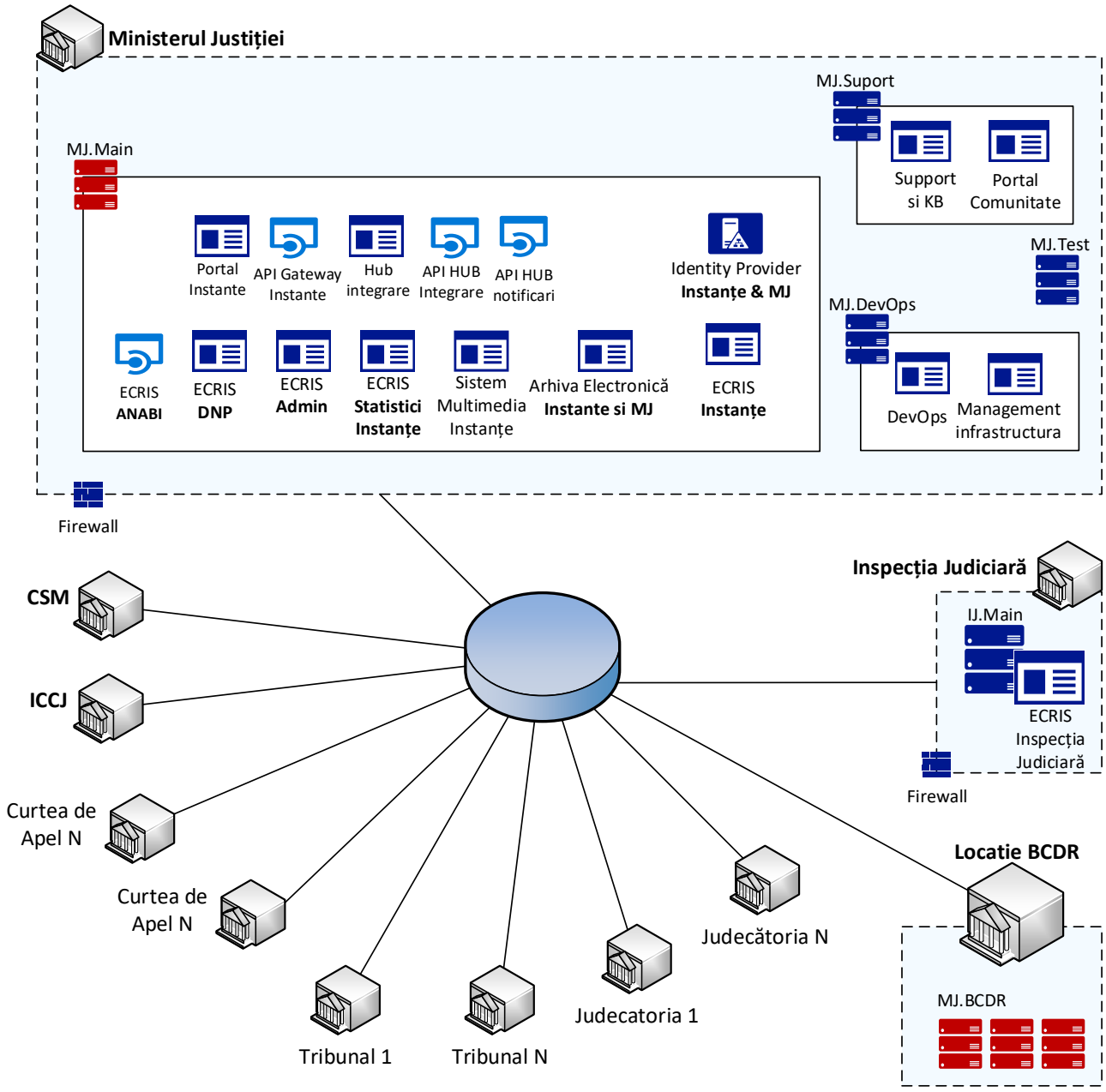
ECRIS Instanțe este aplicația principală folosită de Instanțele din România. Aplicația gestionează dosarele de instanță și fluxurile de lucru din Instanțe. Utilizatorii acestei aplicații sunt judecătorii, grefierii, registratorii și arhivatorii din Instanțe precum si specialiștii IT (pe componentele de administrare specifice).

În prezent aplicația se află la versiunea 4 fiind instalată local în fiecare instanță de judecată, existând în total 237 de instalări ale aplicației. O descriere a funcționalităților acestei aplicații precum și diagramele bazelor de date se regăsesc în documentația AS-IS si pot fi puse la dispoziția furnizorului în etapa de analiză detaliată.

În noul sistem aplicația ECRIS va fi **integral rescrisă**. Noua versiune 5 va include toate funcționalitățile anterioare care vor fi îmbunătățite. De asemenea la data lansării în producție, conținutul bazelor de date din aplicația curentă va trebui migrat în noua aplicație. Noul sistem va asigura coexistență funcțională dintre ECRIS IV și noul sistem pe perioada în care noul sistem va fi instalat, astfel încât funcționalitățile oferite de ECRIS IV (incluzând, dar nelimitându-se la, transferul de dosare și publicarea pe portal.just.ro) sa fie integral disponibile pe parcursul perioadei de tranziție la noul sistem.

4.3.1 Cerinte tehnice ale aplicatiei ECRIS Instante

4.3.1.1 Diagrama de instalare Ecris Instante



Instalarea aplicației ECRIS Instanțe se va realiza centralizat într-o locație pusă la dispozitie de către Ministerului Justiției, aplicație ce va rula pe hardware propriu. Tribunalele, Curțile de Apel, Judecătoriile, CSM și ICCJ vor accesa aplicația pusă la dispoziție, în această locație centralizată.
Toate instanțele vor avea acces la sistemele comune, respectiv:

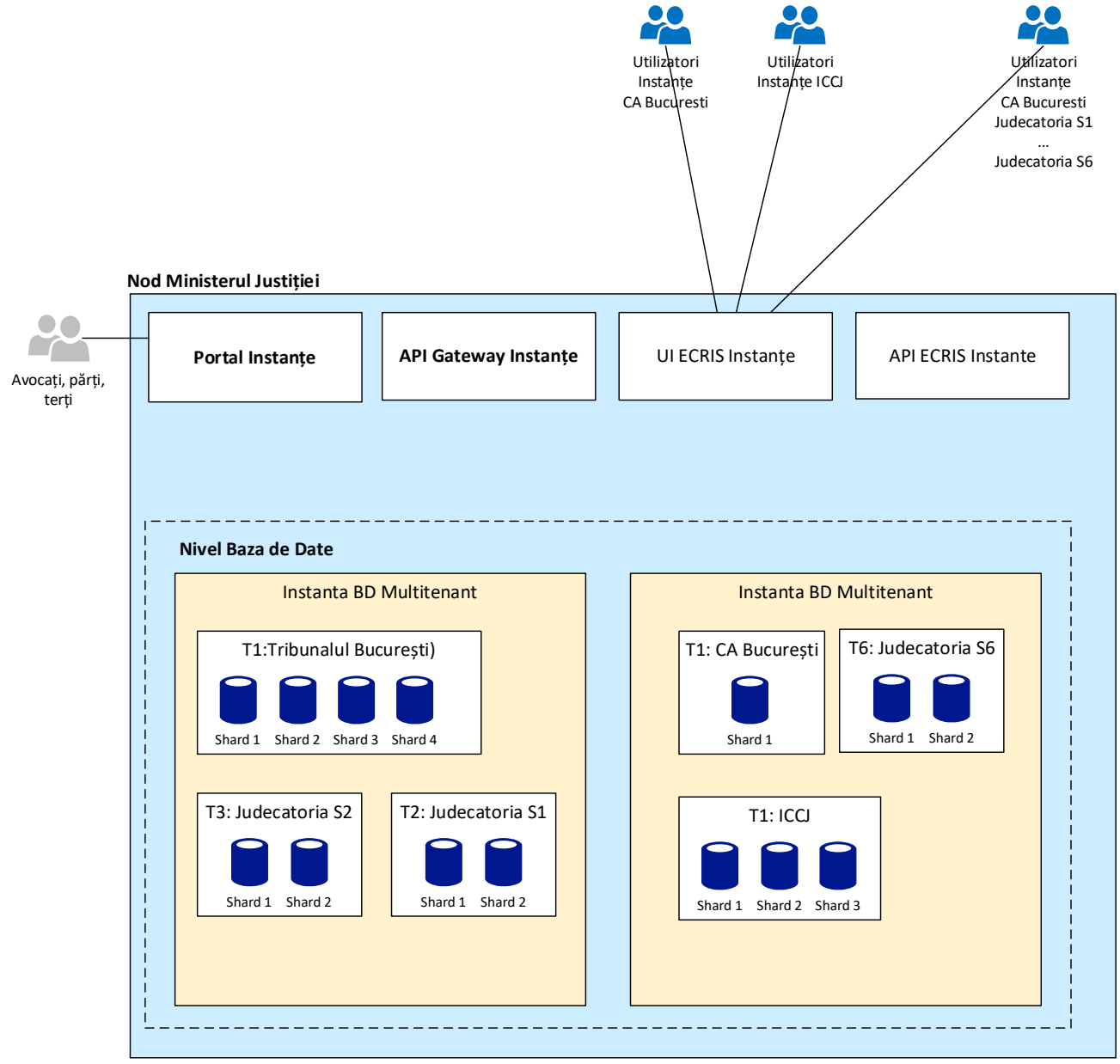
- ECRIS Instante
- Arhiva Electronica instante si MJ
- API Gateway Instanțe (pentru integrarea cu sistemul ECRIS Instanțe)
- HUB Integrare și API-ul Hub-ului de integrare
- Sistem Multimedia Instante
- Sistemul de suport și KB
- Portalul de comunitate

Nodul principal instalat la Ministerul Justitiei va găzdui aplicația ECRIS Instante, Arhiva electronică pentru instanțe și MJ, sistemul de identitate, portalul instantelor, API Gateway-ul aferent, sistemul

multimedia. Acest nod va fi accesat de utilizatorii din instante, de cei din MJ și alte institutii ale sistemului judiciar.
Nodul DevOps va găzdui sistemele necesare pentru DevOps (mediile de dezvoltare, testare, acceptanta, configurare etc.).
Nodul BCDR va găzdui echipamentele și aplicatiile care vor asigura continuitatea și recuperarea în caz de dezastru pentru sistemele instalate în cadrul MJ.
Detaliile tehnice pe care aplicatia ECRIS V trebuie sa le inteplinească sunt descrise în cadrul următoarelor componente:

- Arhitectura Conceptuala,
- Arhitectura Software,
- Cerinte non-functionale,
- ECRIS Application FRAMEWORK
- ECRIS UI FRAMEWORK.

Sistemul ECRIS Instanțe va fi un sistem centralizat de tip multi-tenant, multi-shard, N-tier. Aceasta arhitectură este prezentată în imaginea de mai jos.



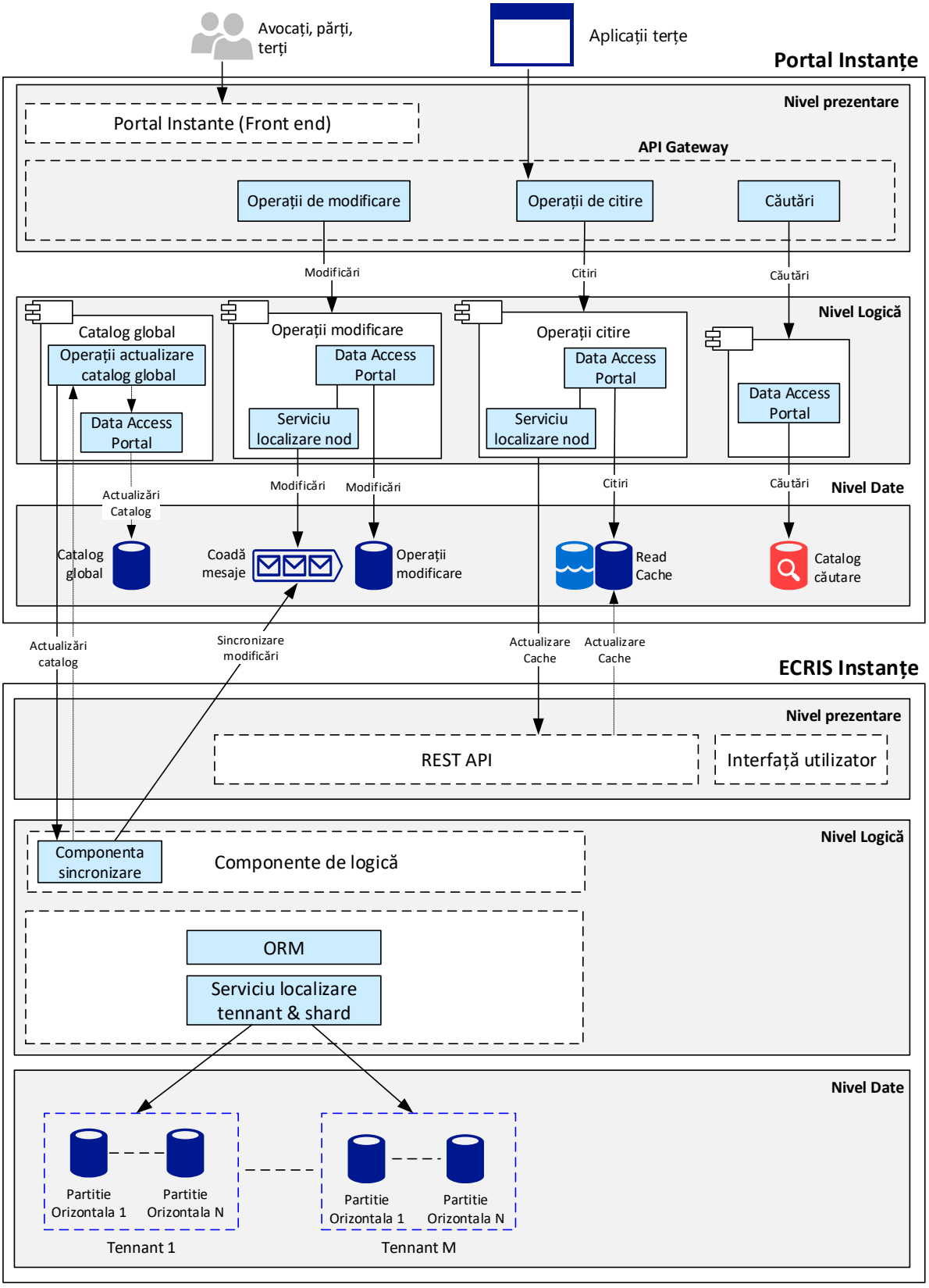
Aplicația ECRIS Instanțe va fi instalată pe un nod central găzduit în cadrul Ministerului de Justiție, nod central ce va găzdui mai multe noduri virtuale, pe care va rula aplicația ECRIS Instanțe. Fiecare nod virtual va fi un sistem de tip multitenant, respectiv va putea găzdui datele mai multor Instanțe de judecată. De asemenea fiecare tenant va suporta partiționarea orizontală a datelor (sharding) în funcție de nevoi. Modulele principale ale aplicației ECRIS Instanțe vor putea fi distribuite pe mai multe echipamente fizice/virtuale (N-tier) în funcție de încărcarea fiecărei instituții.
În practică arhitectura va asigura un nivel de virtualizare la nivel de aplicație și instituție, ceea ce va permite flexibilitate pe mai multe planuri și diferite tipologii de instalare, astfel:

La nivel de nod
Mai multe Instanțe de judecată vor putea folosi același nod virtual.
Pentru a asigura scalabilitatea sistemului, toate modulele aplicației vor putea fi distribuite pe sisteme diferite (orizontal). Spre exemplu interfața utilizator va putea fi distribuită pe sisteme diferite. În mod similar logica aplicației sau bazele de date vor putea fi distribuite în funcție de încărcarea pe fiecare componentă.

La nivel de tenant
Fiecare tenant din cadrul unui nod virtual va putea folosi una sau mai multe partiții orizontale în funcție de volumul de informații, ceea ce va permite scalabilitatea sistemului la nivel de instanță de judecată pe măsură ce volumul de informații din cadrul unei Instanțe crește. Spre exemplu, în cazul în care volumul de informații din cadrul unei Instanțe de judecată crește foarte mult, administratorii sistemului vor putea decide partiționarea datelor pentru distribuirea încărcării. În cazul unei modernizări de hardware administratorii vor putea de asemenea să unească două partiții distincte.

4.3.1.2 Distribuția și localizarea informațiilor Instanțelor

Informațiile legate de dosarele de judecată reprezintă majoritatea informațiilor ce vor fi stocate în bazele de date ale aplicației ECRIS Instanțe, aplicație care va fi instalată pe un nod central, într-o arhitectură virtualizată alcătuită din mai multe noduri virtuale. La un moment de timp un dosar se află pe rolul unei singure Instanțe de judecată și toate informațiile legate de un dosar se află în contextul acelui dosar, având puține relații externe, fapt ce permite distribuirea dosarului și a informațiilor asociate pe mai multe noduri fizice și în mai multe baze de date și partiții orizontale (sharding) cu consecințe rezonabile asupra complexității întregului sistem și beneficii considerabile în privința performanței și a scalabilității.
Având în vedere distribuția datelor pe mai multe noduri este foarte important ca în orice moment să fie cunoscută sursa principală a datelor (single truth).
Ca **regulă general aplicabilă, toate informațiile legate de dosarele de judecată vor fi stocate în bazele de date ale aplicației ECRIS Instanțe (metadate și documente)**.
În baza de date a portalului va exista doar o clonă a informațiilor pentru citire (cache) ce va fi actualizată în funcție de diferite politici de actualizare. De asemenea în baza de date a portalului va fi păstrat un istoric al operațiilor externe realizate de utilizatori (ex: depunerea unui nou document electronic).
În imaginea de mai jos este prezentată conceptual integrarea dintre Portalul Instanțelor și aplicația ECRIS Instanțe.



Figură 2 - integrarea dintre ECRIS Instanțe și Portal Instanțe

Pentru distribuirea datelor pe noduri, tenant și partiții este necesar ca la nivelul fiecărui obiect persistat în sistem să se cunoască locația acestuia. În acest sens la nivelul API Gateway va fi implementat un serviciu care va determina nodul pe care se află un anumit obiect. Pentru acest serviciu se va implementa un catalog global de obiecte care va indica nodul de stocare. Acest catalog

este de asemenea necesar pentru implementarea funcțiilor de căutare globale, astfel pe lângă locația fiecărui obiect (nod/tenant) catalogul va conține și metadatele necesare pentru implementarea căutărilor.
La nivelul fiecărui nod, la nivel de Data Access se va folosi o componentă similară pentru localizarea tenant-ului și a shard-ului în care obiectul se află. Strategia de sharding va fi stabilită în faza de design detaliat, existând multiple posibilități precum distribuirea în funcție de anul dosarului (un shard va stoca unul sau mai mulți ani), caz în care strategia de sharding poate fi de asemenea statică pe baza anului dosarului.
IMPORTANT: serviciul de localizare a unei partiții/shard este prezentat conceptual în documentul de arhitectură, însă în faza de design detaliat, este foarte recomandată utilizarea unor tehnologii existente și/sau facilități oferite de sistemul de baze de date folosit pentru implementarea sistemului, spre exemplu Elastic Database Client Library, Oracle Sharding/RAC sau tehnologii echivalente. NU este recomandată implementarea logicii de sharding la nivelul aplicației. Această recomandare nu se referă la serviciul de localizare a nodurilor pentru care este necesară implementarea la nivelul API Gateway.

4.3.1.3 Interogări multishard

O provocare a unui sistem care folosește sharding o constituie interogările multishard, respectiv interogări care returnează informații din mai multe shard-uri. Acestea nu pot fi complet evitate, însă pot fi reduse la design-ul detaliat prin design-ul API-ului și al interfeței utilizator. În cadrul unui tenant interogările multishard vor fi rezolvate la nivelul componentelor data acces.

4.3.1.4 Comunicarea inter-tenant

Există multiple funcționalități pentru care este necesară comunicarea între doua Instanțe de judecată (tenants) aflate pe același nod (inter-tenant). Un bun exemplu ar fi transferul unui dosar la altă instanță în cazul căilor de atac.
Pentru aceste cazuri, comunicarea inter-tenant (între Instanțele de judecata) va fi rezolvată la nivelul componentelor de business logic sau via API-ul nodului.

4.3.1.5 Operații de actualizare a catalogului global de obiecte

Actualizarea catalogului global de obiecte se va face prin intermediul unei componente de logică implementată în API Gateway. Această componentă va sonda la anumite perioade de timp toate nodurile pentru a actualiza catalogul global cu obiectele noi și modificate. La nivelul nodului, se va implementa o logică care va indica obiectele modificate (spre exemplu, prin folosirea de timestamps). Componenta de sincronizare va implementa o logică care va determina obiectele modificate (spre exemplu de la ultimul apel al nodului central).
Având în vedere că metadatele disponibile pentru căutare reprezintă un set redus de metadate (număr dosar, părțile, hotărârile pe scurt etc) controlul modificărilor nu presupune o complexitate foarte mare.
Pentru siguranță este necesar și un mecanism de reconstruire a catalogului global. Un astfel de mecanism va fi necesar pentru a putea repara eventualele inconsistențe care apar între catalogul global și noduri. De asemenea, mecanismul de reconstruire va fi necesar în cazul mutării anumitor tenants de pe un nod pe altul.

4.3.1.6 Documentație tehnică AS-IS

Documentația tehnica AS-IS referitoare la ECRIS IV Instanțe este descrisă în cadrul livrabilelor din setul L1.3, descrise mai jos. Aplicația ECRIS IV este descrisă la nivel funcțional (fluxuri de lucru și ecrane utilizator) dar și la nivel tehnic (descrieri ale bazelor de date utilizate la nivel de câmp).

- **L1.3-AS-IS Instante-Baze de Date.pdf** – descriere baze de date, tabele și câmpuri asociate (tip de date, valori posibile, descrieri)
- **L1.3-AS-IS Instante-Diagrame ecris_cdms.pdf** – diagrama bazei de date ecris_cdms
- **L1.3-AS-IS Instante-Diagrame ecris_cdms_archive.pdf** - diagrama bazei de date ecris_cdms_archive
- **L1.3-AS-IS Instante-Diagrame ecris_cdms_info.pdf** - diagrama bazei de date ecris_cdms_info
- **L1.3-AS-IS Instante-Diagrame ecris_log.pdf** - diagrama bazei de date ecris_cdms_log

4.3.2 Cerințe funcționale specifice ale aplicației ECRIS Instanțe

4.3.2.1 Documentație funcțională AS-IS

Documentația AS-IS referitoare la functionalitățile ECRIS IV Instanțe este descrisă în cadrul livrabilelor din setul L1.3. Aplicația ECRIS IV este descrisă la nivel functional (fluxuri de lucru și ecrane utilizator) în documentele:

- **L1.3-AS-IS Instante-Aplicatie.pdf** – descriere funcțională aplicație ECRIS IV (descriere fluxuri de lucru și interfețe utilizator)
- **L1.3-AS-IS Instante-Ghid ECRIS 4 civil via Norway 2014** – document suport folosit ca manual de instruire pentru ECRIS IV (documentează fluxurile de lucru din aplicație).

4.3.2.2 Elemente de context, cerinte de business si functionalitati

Informatiile referitoare la Elemente de context, cerințe de business și functionalități ECRIS V Instante sunt descries in cadrul livrabilului **L1.2-Instante-Elemente de context cerințe de business și funcționalități cheie ale sistemului.pdf.** Acest document este însoțit de o serie de diagrame support:

- **L1.2-Instanțe-Diagrama entitatilor.pdf** – diagrama entităților de business din cadrul sistemului.
- **L1.2-Instanțe-Diagrame de process.pdf** – diagrame aferente proceselor de business specifice din cadrul sistemului.
- **L1.2-Instante-Diagrama de context.pdf -** diagrame care descriu contextul aplicției ECRIS Instanțe

4.3.2.3 Specificatiile functionale ale ECRIS V Instante

Cerintele functionale pe care aplicatia ECRIS V Instanțe sunt descrise în cadrul livrabilului **L2 - Instante - Specificatii functionale v1.1.pdf** care este însoțit de o serie de documente suport:

- **L2 - Instante - Model de date detaliat.pdf** – modelul de date al sistemului propus
- **L2 - Instante - Fluxuri Integrare v1.1.pdf** – fluxuri de integrare cu instituții/sisteme externe
- **L2 - Instante - Business Object Model.pdf -** diagrama obiectelor de business
- **L2 - Instante - Use case diagram.pdf -** diagrame de use-case-uri
- **L2 - Rapoarte - Specificatii functionale.pdf -** specificații pentru registre și rapoarte specifice
- **Machete Documente.zip -** machete de documente generate de instanțe, organizate după specific.

4.3.2.4 Mecanismul de Distribuire Aleatoare a Dosarelor

O functionalitate extrem de importanta specifica aplicației ECRIS Instanțe este mecanismul de Distribuire Aleatoare a Dosarelor. Detaliile funcționale sunt descrise in cadrul livrabilului **L2 - Instante - Specificatii functionale v1.1.pdf** – capitolul 2.6. Prin prisma dinamicității sale, acest mecanism trebuie sa fie cât mai parametrizabil și flexibil, având un caracter specific in funcție de sectie si chiar de institutie. Detalierea acestui mecanism va face obiectul unei analize specifice în etapa de Analiză Detaliată.

4.3.3 Dosarul electronic ECRIS Instanțe (eDosar)

O funcționalitate majoră a noii aplicații este dosarul electronic care va permite Instanțelor o gestiune integral electronică a documentelor din dosare. De asemenea aplicația ECRIS Instanțe va fi integrată cu aplicația ECRIS Portal Instanțe și va permite ca orice interacțiune cu Instanțele să se deruleze integral online.
Cerintele tehnice pe care Dosarul electronic ECRIS V trebuie sa le indeplineasca sunt descriese in cadrul Componentei **Stocarea și accesul la documentele electronice.**
Cerintele funcționale legate de Dosarul electronic ECRIS Instante se regasesc in cadrul livrabilului **L2 - Portal Instante - Specificatii functionale.pdf**, care este însoțit de documentul **L2 - Portal Instante - Use case diagram.pdf**

4.3.3.1 Informații volumetrice

In tabelul de mai jos sunt sintetizate câteva informații relevante pentru o privire de ansamblu.

Parametru	Valoare
Parametri generali	
Dimensiune stocare / pagina document (MB)	**0.125**
Instanțe	
Utilizatori interni (total angajați din schema de personal)	**12,781**
Nr de request-uri externe / zi. Estimarea se bazează pe traficul actual al portalului Instanțelor înmulțit cu 3, având în vedere ca noul portal va permite și interacțiunea online	**3,000,000**
Medie de dosare noi în fiecare an	**2,117,796**
Cauze soluționate anual	**2,170,715**

4.3.3.2 Sistem de stocare si redare Video / Multimedia

Sistemul va asigura stocarea centralizată a înregistrărilor de audieri și a altor materiale video și audio depuse de parchete sau instanțele de judecată în dosarul electronic de instanță. Documentele electronice din dosarul electronic al Instanței vor fi persistate în bazele de date ale aplicației ECRIS Instanțe, cu excepția înregistrărilor video și audio. Acestea vor fi stocate centralizat, din cauza volumului potențial foarte mare de informații și pentru a eficientiza costurile cu achiziția de echipamente hardware.
Acest sistem va asigura persistența înregistrărilor audio și video și integrarea cu aplicația ECRIS Instanțe. În cadrul ECRIS Instanțe, înregistrările video și audio vor fi parte din dosarul electronic cu singura deosebire că vor fi stocate centralizat. Sistemul trebuie să ofere posibilitatea de streaming

video și audio , astfel încât un utilizator al aplicației ECRIS Instanțe (judecător/grefier) să poată accesa foarte ușor o înregistrare video sau audio, fără a fi nevoit să descarce integral fișierul pe calculatorul propriu.
Sistemul trebuie să asigure și transformarea (encoding) fișierelor multimedia într-un format potrivit pentru streaming multimedia (ex: H.264 sau H.265 preferabil datorită compresiei mai bune). Standardul de compresie va fi stabilit în perioada de implementare.
Sistemul trebuie să permită integrarea cu sistemul de video-conferințe al instanțelor. Această integrare este descrisă în documentul **L2 – Instante – Fluxuri Integrare v1.1.pdf – Capitolul 16**

IMPORTANT: din motive legale, în cazul fișierelor video și audio ce vor fi convertite la un standard comun, sistemul va păstra și originalul. De asemenea sistemul trebuie să permită semnarea și marcarea temporară a conținutului pentru a se împiedica alterarea acestora.
NOTĂ: Nodul video/multimedia a fost identificat ca nod separat în scenariul de arhitectură distribuit, pentru a permite stocarea centralizată a conținutului video în scopul economisirii de spațiu de stocare. Sistemul video/multimedia este o extensie a dosarului electronic, astfel stocarea conținutului multimedia se poate face folosind același sistem de persistare al fișierelor ce urmează să fie folosit și pentru restul documentelor din dosarul electronic, cu deosebirea că pentru fișierele multimedia va fi necesară implementarea funcționalităților suplimentare descrise mai sus (encoding, streaming etc.).
Cerințele tehnice pe care Sistemul de stocare si redare Video / Multimedia trebuie sa le îndeplinească sunt descrise in cadrul Componentei **Stocarea si accesul la documentele electronice**.

4.3.4 Nomenclatoare ECRIS Instanțe

O componentă importantă a functionalităților ECRIS Instante o reprezintă Nomenclatoarele specifice. Aceste nomenclatoare sunt descrise in cadrul documentului **L2 - Instante - Model de date detaliat.pdf**. Administrarea nomenclatoarelor este descrisă în documentul **L2 - Instante - Specificatii functionale v1.1.pdf – Capitolul 2.11**
De asemenea, există o serie de nomenclatoare comune între ECRIS Instante și Ecris Parchete care trebuiesc implementante și administrate în mod unitar. Aceste nomenclatoare sunt descrise în cadrul documentului **L2 - MJ - Model de date detaliat.pdf - Capitolul 2.4.** Administrarea acestor nomenclatoare centralizate este descrisă în documentul **L2 - MJ - Specificatii functionale.pdf – Capitolul 2.2**

4.3.5 Rapoarte ECRIS Instante

Pentru raportare se vor folosi baze de date distincte, astfel încât interogările de raportare să nu afecteze performanța aplicațiilor principale. În funcțiile de cerințele de raportare ale aplicației, bazele de raportare pot fi replici OLTP peste care opțional se pot construi baze de date OLAP. Implementarea de baze de date OLAP este recomandată cel puțin pentru aplicațiile de Statistici, ECRIS Instanțe și ECRIS Parchete.
Rapoartele aferente ECRIS Instante care vor fi disponibile instantelor, sunt impartite in doua categorii:

4.3.5.1 Rapoarte Operationale Instante

Rapoartele Operationale Instante sunt rapoarte predefinite care vor putea rula direct pe baza de date ECRIS Instante. Aplicația va oferi un modul de raportare comun pentru toate Instanțele de judecată, fiind bazat pe o bază de date comună care include date înregistrate în aplicațiile ECRIS Instanțe. Accesul la rapoarte este limitat printr-un sistem de roluri și permisiuni.
În functie de informatiile continute de acestea, unele dintre acestea nu vor putea fi rulate decat de persoane cu drept de administrator pentru instanta/instantele respective.
Cerintele tehnice generale de realizare/optimizare a acestor rapoarte se regasesc in cadrul documentului **L2.4. Specificatii tehnice ale componentelor hardware si software.pdf – capitolul 4.5**.
Detaliile funcționale ale acestor rapoarte sunt descrise in cadrul livrabilului **L2 - Rapoarte - Specificatii functionale.pdf – Capitolele 2.3, 2.6, 2.7**

4.3.5.2 Rapoarte Statistice Instante

Modul de acces și generare a rapoartelor Statistice Instanțe este descrisă în cadrul componentei Statistică Judiciară.
Aplicația va oferi un modul de raportare comun pentru toate Instanțele de judecată, fiind bazat pe o bază de date comună care include date înregistrate în aplicațiile ECRIS Instanțe. Accesul la rapoarte este limitat printr-un sistem de roluri și permisiuni.
În functie de informațiile conținute de acestea, unele dintre acestea nu vor putea fi rulate decat de persoane cu drept de administrator pentru instanta/instantele respective.
Detaliile functionale ale acestor rapoarte sunt descrise in cadrul livrabilului **L2 - Rapoarte - Specificatii functionale.pdf – Capitolele 2.4 și 2.5**

4.3.6 Integrari ECRIS Instante

Integrările necesare sistemului ECRIS sunt enumerate în documentul „2.2.1.B – Integrări între sisteme" parte din livrabilul 2.2.1 – Cerințe non-funcționale. Prin integrare înțelegem conectarea directă, la nivel tehnic, dintre două sisteme informatice cu scopul de a schimba informații relevante pentru ambele sisteme.
Integrările dintre aplicațiile sistemului ECRIS se împart în două categorii:
- Integrările dintre aplicațiile sistemului ECRIS .
- Integrări dintre aplicații ale sistemului ECRIS și aplicații externe.

Prin aplicație externă înțelegem orice aplicație ce nu face parte din scopul sistemului ECRIS, inclusiv aplicații operate de instituții din sistemul de justiție.
Toate integrările necesare sunt enumerate în documentul L2.2.1.B – Integrari intre sisteme.xlsx (sublivrabil al livrabilului 2.2.1 – Cerinte non-functionale). Detalierea acestor integrări se regăsește în documentul **L2 - Instante - Fluxuri Integrare v1.1.pdf.**

Cerintele tehnice generale sunt prezentate in cadrul componentei Integrări

4.3.6.1 Integrari ECRIS Instante cu componentele interne ECRIS 5 (inclusiv Portaluri)

4.3.6.1.1 API Gateway Instanțe

Componenta API Gateway a Instanțelor va fi punctul unic de interacțiune dintre alte aplicații și ECRIS Instanțe. Aceasta este componenta cheie pentru integrarea facilă a sistemului ECRIS cu alte sisteme.

API Gateway va agrega toate API-urile disponibile la nivelul Instanțelor și va redirecționa apelurile către API-ul corespunzător. De asemenea API Gateway va asigura accesul securizat, autentificând și autorizând apelanții.
Așa cum este menționat mai sus, portalul instanțelor va utiliza componenta API Gateway. Din acest punct de vedere portalul trebuie privit ca orice alta aplicație terță care se integrează cu ECRIS Instanțe.
Integrarea dintre celelalte aplicații ale sistemului de justiție și ECRIS Instanțe se va face prin API Gateway. în mod special integrarea dintre ECRIS Parchete și ECRIS Instanțe se va realiza prin componentele API gateway ale celor două aplicații. Trebuie subliniat faptul că toate integrările între alte aplicații și ECRIS Instanțe vor fi realizate prin API Gateway. Spre exemplu integrarea la nivel de baze de date intre ECRIS Instanțe și ECRIS Parchete nu este permisă.
Cerintele tehnice generale sunt detaliate in cadrul componentei Integrari

4.3.6.1.2 Integrare ECRIS Instante cu ECRIS Parchete (PICCJ/DNA/DIICOT)

Detaliile functionale ale acestei integrări sunt descrise in cadrul livrabilului L2 - Parchete - Integrări Subcapitolul 3.1

4.3.6.1.3 Integrare ECRIS Instante cu sitemul de inregistrare audio

Afișarea de informații referitoare la ședințele în desfășurare este descrisă ca parte din documentul **L2 - Portal Instante - Specificatii functionale.pdf - Secțiunea 2.1.2** sub formă de pagină web dinamică, care poate fi redată pe orice fel de dispozitiv TV / info-chiosc (cu browser web integrat).

4.3.6.1.4 Integrare ECRIS Instante cu Portal Instante

API Gateway va agrega toate API-urile disponibile la nivelul Instanțelor și va redirecționa apelurile către API-ul corespunzător. De asemenea API Gateway va asigura accesul securizat, autentificând și autorizând apelanții.
Așa cum este menționat mai sus, portalul instanțelor va utiliza componenta API Gateway. Din acest punct de vedere portalul trebuie privit ca orice altă aplicație terță care se integrează cu ECRIS Instanțe.
Cerintele de integrare specifice sunt detaliate in livrabilul **L2 - Portal Instante - Specificatii functionale.pdf**

4.3.6.1.5 Integrare ECRIS Instante cu Inspectia Judiciara

Cerintele de integrare specifice sunt detaliate in livrabilul L2 - IJ - Specificatii functionale - faza II Subcapitolul 2.3

4.3.6.1.6 Integrare ECRIS Instante cu DNP (Probatiune)

Cerintele de integrare specifice sunt detaliate in livrabilul **L2 - Probatiune - Specificatii functionale.pdf - capitolul 3.1.3**

4.3.6.2 Integrari cu componente externe ECRIS 5

4.3.6.2.1 API Gateway Instanțe

Componenta API Gateway Instanțe va permite extinderea facilă a sistemului ECRIS cu alte aplicații, inclusiv aplicații dezvoltate de terți. Spre exemplu ne putem imagina furnizori externi care dezvoltă aplicații dedicate avocaților pentru managementul dosarelor. Ne putem imagina aplicații mobile, dezvoltate de sistemul de justiție sau de furnizori terți, pentru accesul la informațiile din dosar. Ne putem chiar imagina în viitor o piață deschisă de aplicații (in genul Apple Store/Google Marketplace) pentru aplicații specifice sistemului de justiție.
Detaliile tehnice generale se regasesc in cadrul componentei Integrari/ API Gateway

4.3.6.2.2 Integare ECRIS Instante cu ANABI

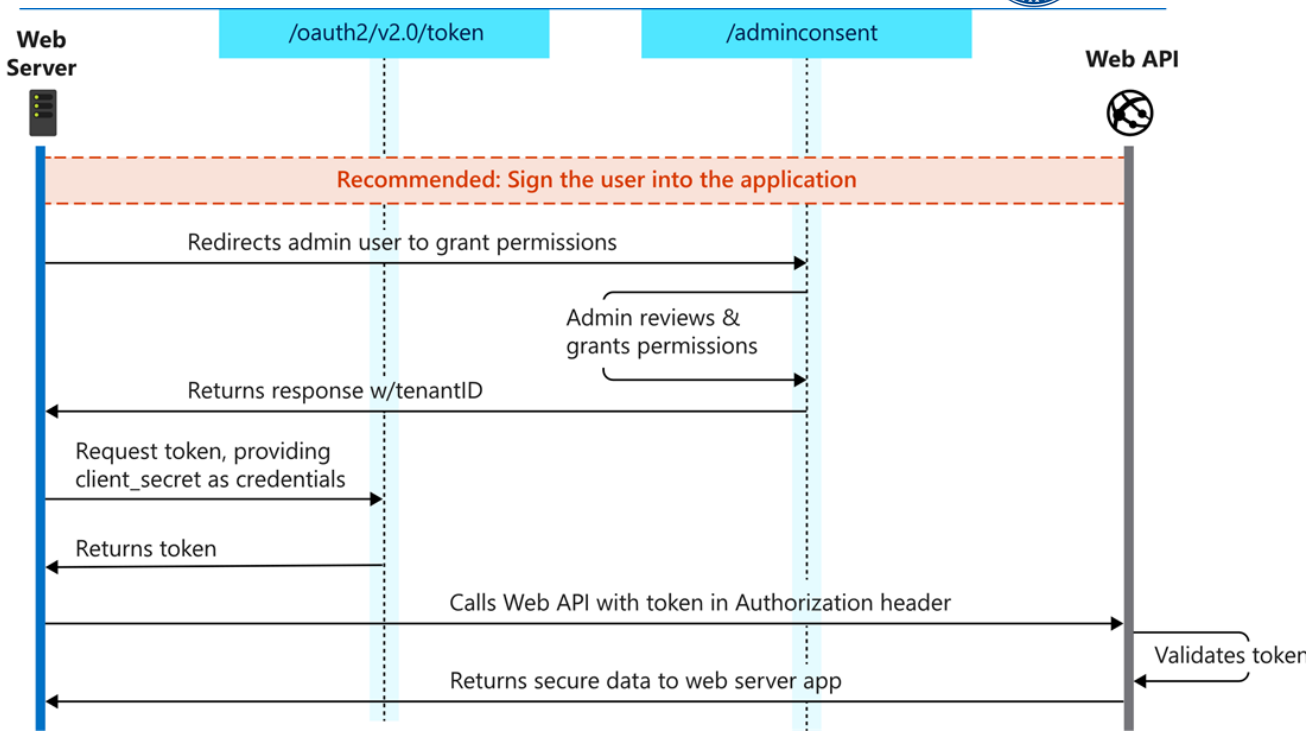
Componenta asigură interfațarea sistemului implementat de ANABI, de evidență a bunurilor sechestrate, confiscate și valorificate în cadrul procesului penal cu aplicațiile ECRIS Parchete și ECRIS Instanțe. Scopul interfațării este de a comunica date despre ordonanțele procurorilor sau hotărârile judecătorești privind bunurile indisponibilizate, precum și detalii referitoare la administrarea și valorificarea acestora. Din punct de vedere tehnic ECRIS ANABI nu este o aplicație distinctă ci o componentă care va asigura integrarea dintre celelalte aplicații ale sistemului ECRIS cu sistemul ANABI care nu face parte din scopul dezvoltării.
Detalierea cerințelor de integrare se regăsesc în livrabilului **L2 - Instante - Specificatii functionale v1.1.pdf – Capitolul 2.10**

4.3.6.2.3 Detalii tehnice de implementare servicii web

Interfațarea dintre aplicațiile ECRIS Instanțe si ANABI va folosi două tipuri de interfețe programatice:

- interfețe funcționale care satisfac cerințele prezentate mai sus
- interfețe suport folosite pentru re-concilierea nomenclatoarelor comune folosite de sistemele integrate

Toate interfețele vor fi de tip Web API. Protocolul de transport este HTTPS.
Standardul de autentificare este bazat pe fluxul OAuth2 client credentials flow. Un exemplu este furnizat in diagrama de mai jos, în care Web Server este aplicația care apelează API-urile de interfațare.



Payload-urile transmise vor fi bazate pe un model de date agreat de comun acord si vor conține acolo unde este posibil cheile de business asociate nomenclatoarelor din sistemul țintă.

4.3.6.2.4 Integrare ECRIS Instante cu Registrul ONG

Aplicația ține o evidență centralizată a persoanelor juridice fără scop patrimonial și a beneficiarilor reali ai acestora, totodată oferind instrumente de verificare disponibilitate a denumirilor, respectiv rezervare la cerere.
Detalierea cerintelor de integrare se regasesc in livrabilului/livrabilelor **L2 - RNONG- Specificatii functionale.pdf**

4.3.6.2.5 Integrare ECRIS Instante cu alte sisteme (pentru care exista informatii detaliate)

Detalierea cerințelor de integrare se regasesc in livrabilului **L2 - Instante - Fluxuri Integrare v1.1.pdf**

4.3.7 Arhiva Electronica ECRIS Instante

Aplicația de arhiva electronica va asigura arhivarea permanentă a informațiilor din aplicațiile sistemului ECRIS cu excepția aplicațiilor dedicate parchetelor care vor beneficia de o componentă de arhivare dedicată. Aplicația de arhivare va fi folosită de Instanțele de judecata, CSM, Inspecția Judiciară, Ministerul Justiției și instituțiile subordonate (ANABI, DNP). Informațiile arhivate vor fi stocate pe echipamente specializate tip WORM.

4.3.7.1 Arhivarea Logica ECRIS Instante:

În cadrul sistemului ECRIS vor fi prevăzute două tipuri de arhivare: logică și permanentă. Arhivarea logică va păstra informațiile în sistemele de stocare online iar informațiile arhivate vor fi marcate

logic ca fiind arhivate (flag de arhivare). Arhivarea permanentă va presupune transferarea efectivă a datelor în sisteme de arhivare dedicate cu caracteristici WORM.
IMPORTANT: pentru arhivarea logică datele vor fi păstrate în aceleași tabele și baze de date, dar vor fi marcate logic ca fiind arhivate, respectiv datele NU vor fi transferate în alte tabele sau baze de date dedicate arhivei logice. Transferul datelor arhivate logic în cadrul aceleiași baze de date generează în timp complexitate nenecesară care nu poate fi ușor controlată și din acest motiv această abordare NU este recomandată. Această abordare a fost folosită în ECRIS 4 și versiunile anterioare unde și-a dovedit ineficacitatea. Astfel datele arhivate logic vor fi păstrate în aceleași tabele cu datele nearhivate, iar filtrarea se va realiza prin intermediul unor structuri de tip view (recomandat) sau la nivel de logică de aplicație. Pentru aplicațiile care folosesc sharding, este recomandat ca datele arhivate să fie persistate în shard-uri dedicate arhivei logice pentru a descărca bazele de date online, cu condiția ca distribuirea să facă parte din strategia normală de sharding. Altfel spus, este esențial ca datele arhivate logic să NU primească un tratament separat în logica aplicației (în afara eventualei filtrări logice), respectiv o interogare (query) care cuprinde atât date nearhivate cât și date arhivate logic nu trebuie să fie cu nimic diferită față de o interogare care cuprinde doar date nearhivate sau doar date arhivate. În eventualitatea în care datele arhivate sunt stocate în shard-uri separate, un astfel de query va fi rezolvat prin mecanismul general de interogare multi-shard, în mod transparent pentru componentele de logică ale aplicației.
Detaliile tehnice generale pentru aceste functionalitati se regasesc descrise amănunțit în cadrul componentei Arhiva Electronică.

4.3.7.2 Arhivarea Permanenta ECRIS Instanțe:

Aplicația de arhiva electronică va asigura arhivarea permanentă a informațiilor din aplicațiile sistemului ECRIS cu excepția aplicațiilor dedicate parchetelor care vor beneficia de o componentă de arhivare dedicată. Informațiile arhivate vor fi stocate pe echipamente specializate tip WORM.
Detaliile tehnice generale pentru aceste funcționalități se regăsesc detaliate în cadrul componentei Arhiva Electronică.

4.3.8 Cerinte de Securitate ECRIS Instante

Cerințele tehnice generale sunt detaliate in cadrul componentei Cerințe de Securitate
Cerințele de Securitate sunt împărțite in trei categorii:

4.3.8.1 Securitatea stocarii si auditarii datelor/documentelor ECRIS Instante

Cerințele specifice pentru ECRIS Instanțe sunt detaliate în cadrul livrabilului **L2.2.1.A-Cerinte non-functionale ale sistemului.pdf – Capitolul 2.1.2**

4.3.8.2 Securitatea accesului la date/documente ECRIS Instante

Cerintele specifice pentru ECRIS Instante sunt detaliate in cadrul livrabilului **L2.2.1.A-Cerinte non-functionale ale sistemului.pdf – Capitolul 2.1.2**

4.3.8.3 Sistem de identitate (Identity Provider) Ecris Instante

Pentru autentificarea utilizatorilor și aplicațiilor în cadrul sistemului ECRIS Instanțe este necesară implementarea unui **sistem de identitate (Identity Provider).** Acest sistem va fi un sistem de tip Single Sign-On pentru toate aplicațiile dezvoltate în cadrul sistemului ECRIS. Sistemul va permite ca utilizatorii să poată folosi un singur cont de utilizator pentru a accesa orice aplicație din sistemul ECRIS, în funcție de drepturile pe care le au.
Acest sistem trebuie să implementeze cel puțin un standard deschis de autentificare (spre exemplu OAuth 2.0) astfel încât integrarea cu aplicațiile dezvoltate să fie ușor de realizat. Toate aplicațiile din sistemul ECRIS vor folosi serviciile sistemului de identitate pentru autentificarea utilizatorilor și nu vor implementa propriile mecanisme de autentificare. Autorizarea accesului la resurse va fi implementată la nivelul fiecărei aplicații și API.
Sistemul trebuie să ofere facilități clasice de înregistrare, resetare a parolei etc. precum și posibilitatea autentificării de tip multi-factor (ex: parolă și SMS / email). Sistemul trebuie să permită posibilitatea de a asocia un certificat digital contului unui utilizator (respectiv asocierea cheii publice cu un cont). Această funcție este necesară pentru asigurarea funcționalității de validare a semnăturilor electronice. De asemenea pentru utilizatorii care dețin un certificat digital, acesta ar trebui să poată fi folosit inclusiv pentru autentificare.
Sistemul trebuie să ofere funcționalități de validare a identității. Această cerință este necesară pentru a valida identitatea terților care vor interacționa online prin intermediul portalului. Procesul de validare a identității este descris în cerințele funcționale.
Cerințele specifice pentru ECRIS Instanțe sunt detaliate în cadrul livrabilului **L2.2.1.A-Cerinte non-funcționale ale sistemului.pdf – Capitolul 2.1.2**

4.3.8.4 Securitatea transferului datelor/documentelor ECRIS Instante

Cerințele specifice pentru ECRIS Instanțe sunt detaliate în cadrul livrabilului **L2.2.1.A-Cerinte non-functionale ale sistemului.pdf – Capitolul 2.1.2**

4.3.9 Cerinte non-functionale legate de ECRIS Instante

Cerintele non-funcționale generale ale sistemului ECRIS sunt detaliate în cadrul componentei Cerințe non-funcționale.
Cerintele non-funcionale specifice ECRIS Instanțe (inclusiv cele volumetrice) sunt detaliate în cadrul livrabilului **L2.2.1.A-Cerinte non-funcționale ale sistemului.pdf – Capitolul 2.1.2**

4.3.10 Administrare ECRIS Instanțe

Cerințele tehnice generale se regăsesc în cadrul Componentei Administrare Sistem ECRIS.
Componentele principale ale acestui modul sunt urmatoarele:

4.3.10.1 Atribuire/Definire Roluri Utilizator si drepturi specifice de acces ECRIS Instante

Cerințele tehnice sau funcționale specifice ECRIS Instanțe sunt detaliate în cadrul livrabilului **L2 - Instante - Specificatii functionale v1.1.pdf – capitolul 2.11**

4.3.10.2 Administrare Nomenclatoare Specifice ECRIS Instante

Cerințele tehnice sau funcționale specifice ECRIS Instanțe sunt detaliate în cadrul livrabilului **L2 - Instanțe - Specificații funcționale v1.1.pdf - capitolul 2.11**

4.3.10.3 Adiministrare si Generare Rapoarte (operationale sau statistice) ECRIS Instante

Cerințele tehnice sau funcționale specifice ECRIS Instanțe sunt detaliate în cadrul livrabilului **L2 - Instante - Specificatii functionale v1.1.pdf - capitolul 2.11**

4.3.10.4 Administarea repartitiei aleatoare a dosarelor ECRIS Instante

Cerințele tehnice sau funcționale specifice ECRIS Instanțe sunt detaliate în cadrul livrabilului **L2 - Instanțe - Specificații functionale v1.1.pdf - capitolul 2.6**

4.3.10.5 Alte Cerinte de Administrare specifice ECRIS Instante

Cerințele tehnice sau funcționale specifice ECRIS Instanțe sunt detaliate în cadrul livrabilului **L2 - Instanțe - Specificații funcționale v1.1.pdf - capitolul 2.11**

4.3.10.6 Tranzitie ECRIS Instante

Strategia generala de tranzite la Sistemul ECRIS V este descrisă în cadrul componentei Tranziție.
Elementele specifice ECRIS Instanțe:

4.3.10.6.1 Migrare Date ECRIS Instante

Strategia generală este descrisă în cadrul componentei Tranziție
Cerințe specifice:

4.3.10.6.1.1 Situatia actuala ECRIS Instante

În cadrul instanțelor de judecată pentru evidența dosarelor este folosită versiunea 4 a aplicației ECRIS CDMS Instanțe. Această aplicație este instalată pe un server local în cadrul fiecărei instanțe de judecată. Pentru stocarea documentelor electronice în cadrul instanțelor se folosește și aplicația SAE – Sistem de arhivare electronică (EAS – Electronic Archiving System).
Documentația pentru aplicația ECRIS CDMS Instanțe se găsește în cadrul livrabilului 1.3 Documentatie AS-IS si cuprinde:

- Documentatie AS-IS high-level realizată in cadrul proiectului SIPOCA 55
- Documentație detaliată a bazelor de date folosite de aplicație realizată în cadrul proiectului SIPOCA55
- Ghid de utilizare ECRIS 4
- Diagrame visio ale celor 4 baze de date (CDMS, CDMS_Archive, CDMS_Info si ECRIS_Log)

Documentația pentru aplicația SAE se găsește în cadrul livrabilului 1.3 Documentatie AS-IS si cuprinde:

- Specificația sistemului SAE
- Documentatia bazei de date (HiStoreDB.chm)
- Specificatia tehnica folosita in caietul de sarcini pentru realizarea SAE
- Manualul de utilizare al aplicatiei
- Manualul de administrare al aplicatiei

Informațiile detaliate necesare migrarii ECRIS Instanțe se regăsesc în cadrul livrabilului **L2.2.1.C-Cerințe migrare.pdf**

4.3.10.6.1.2 Scop Migrare ECRIS Instanțe

Migrarea datelor din bazele de date ale instanțelor este cea mai complexă din motive operaționale care țin de numărul bazelor de date care trebuie migrate. Numărul total de instanțe este de 243, dintre care:

- Înalta Curte de Casație și Justiție
- 15 Curți de Apel
- 42 Tribunale
- 4 Tribuale specializate
- 176 Judecătorii
- 1 Curte Militară de Apel
- 4 Tribunale militare

Ținând cont de faptul că activitatea instanțelor de judecată nu poate fi întreruptă pentru perioade foarte lungi de timp, o strategie care să presupună migrarea simultană a tuturor instanțelor ar fi foarte greu de pus în practică din punct de vedere operațional. Astfel este necesară o strategie de migrare treptată a instanțelor.

Pentru a asigura migrarea treptată a instanțelor, migrările se vor efectua în grupuri de instanțe (clustere) formate în jurul curților de apel. Această strategie asigură că majoritatea căilor de atac în cadrul unui grup de instanțe se vor realiza folosind aceeasi versiune de aplicație. Astfel un grup de instanțe va fi format dintr-o curte de apel, tribunalele și judecătoriile arondate. De semenea primul grup de instanțe va conține și Înalta Curte de Casație și Justiție. Migrarea unui grup va fi considerată de succes doar dacă toate migrările instanțelor din grup sunt de succes. În cazul unui eșec procedura de migrare va fi reluată la o dată ulterioară pentru toate instanțele din grup. Rezultă astfel 16 grupuri de instanțe care vor fi migrate:

- Grupul BUCUREŞTI (inclusiv ICCJ)
- Grupul CRAIOVA
- Grupul CLUJ
- Grupul TIMIŞOARA
- Grupul PITEŞTI
- Grupul PLOIEŞTI
- Grupul ALBA IULIA
- Grupul SUCEAVA
- Grupul GALAȚI
- Grupul IAŞI
- Grupul CONSTANȚA
- Grupul BACĂU
- Grupul ORADEA
- Grupul BRAŞOV
- Grupul TÂRGU MUREŞ
- Grupul Militar

Ordinea de migrare va putea fi agreată cu beneficiarul în funcție de constrângerile existente la momentul respectiv.

În cadrul aplicației aflate în producție, utilizatorii au procedat la introducerea datelor folosind caractere cu diacritice specifice tastaturilor Română Tradițional (Legacy) și Română Standard, aspect de care trebuie ținut cont la migrarea datelor din bazele actuale, în vederea afișării corecte a datelor.

Din perspectiva filtrelor, căutarea datelor trebuie să fie “accent-insensitive” și “case-insensitive”, pentru a determina apariția tuturor rezultatelor posibile.

4.3.10.6.1.3 Proceduri de coexistență pentru ECRIS Instanțe

În perioada migrării, diferitele grupuri de instanțe (descrise mai sus) vor rula versiuni diferite de aplicații. Strategia de migrare pe grupuri de instanțe va asigura că pentru majoritatea căilor de atac dosarele vor fi transferate către o instanță din același grup care rulează aceeași versiune de aplicație, respectiv transferul se va realiza în cadrul sistemului. Vor exista însă și situații în care un dosar va fi transferat către o instanță care rulează o versiune diferită de aplicație, mai nouă sau mai veche, ambele scenarii find posibile. Înalta Curte de Casație și Justiție se va afla în această situație teoretică pe toată perioada migrării, deoarece un dosar care a avut fondul la un tribunal care folosește versiunea veche a aplicației, va fi transferat pentru recurs la ÎCCJ care va folosi noua versiune a aplicației.
Pentru a acoperi din punct de vedere procedural aceste situații, furnizorul va elabora un set detaliat de proceduri de coexistență pentru perioada migrării. Aceste proceduri vor acoperi toate situtațiile teoretice care vor putea apărea în perioada migrăii, printre care:

- Recursul (art 483 NCPC)
- Recursul incident și recursul provocat (art 491 NCPC)
- Contestația în anulare (art 503 NCPC)
- Revizuirea (art 509 NCPC)
- Recursul în casație (art 433 NCPP)
- Revizuirea (art 452 NCPP)
- Situațiile de rejudecare
- Situațiile de revizuire care presupun tranferul dosarului
- Etc.

IMPORTANT: procedurile de coexistență pot fi simplificate dacă ulterior migrării, sistemul vechi este menținut pentru a transfera un dosar și apoi se folosesc intrumentele de migrare pentru a migra discret dosarul în noua versiune.
Exemplu: instanța A folosește noua versiune a ECRIS, iar instanța B folosește versiune veche de ECRIS. Un dosar trebuie transferat de la A la B. Instanța A va folosi noua versiune a sistemului, dar va păstra în funcțiune și versiunea vechea. Instanța B va transfera dosarul folosind sistemul vechi. Dosarul va ajunge la instanța A în sistemul vechi. Se vor folosi instrumentele de migrare pentru a migra dosarul din sistemul vechi în noul sistem.
Instrumentele de migrare vor fi utilizabile doar în acest caz, nu si vice-versa (e.g. de la versiune noua, la versiune veche). Pentru aceste situații furnizorul va furniza proceduri manuale.

4.3.10.6.1.4 Acceptanță Migrare ECRIS Instante

Acceptanța migrărilor se va realiza la finalul proiectului, ca parte din procesul general de acceptanță. Criteriile de acceptanță a activității de migrare vor urmări migrarea integrală a datelor din toate bazele de date avute în scop în noile baze de date ECRIS, respectiv:

- Toate bazele de date ECRIS CDMS utilizate de către instanțe
- Toate bazele de date SAE utilizate de către instanțe

Alte detalii referitoare la acceptanta Migrare ECRIS Instante se regasesc in livrabilul L2.2.1.C – Cerințe migrare

4.3.10.6.2 Intruire ECRIS Instante

Strategia generală este descrisă în cadrul componentei Instruire ECRIS Instanțe
Cerințele specifice referitor la Instruire ECRIS Instanțe (personal tehnic și funcțional) se regăsesc în cadrul livrabilului L4.3-Plan de formare.pdf

4.3.10.6.2.1 Instruire Tehnica

Informațiile volumetrice privind necesitatea de instruire a personalului tehnic (Specialisti IT) se regăsesc în livrabilul L4.3-Plan de formare.pdf

4.3.10.6.2.2 Instruire Functionala

Informațiile volumetrice privind necesitatea de instruire a personalului funcțional (Grefieri, Judecatori, etc..) se regăsesc în livrabilul L4.3-Plan de formare.pdf

4.3.10.6.3 Roll-out ECRIS Instante

Strategia generală este descrisă în cadrul componentei Tranziție
Cerințele specifice referitor la Instruire ECRIS Instanțe se regăsesc în cadrul livrabilului L4.3-Plan de formare.pdf

4.4 ECRIS Parchete

Ecosistemul de aplicații disponibil în cadrul parchetelor este structurat în oglindă cu sistemul Instanțelor. Pentru fiecare aplicație există o aplicație echivalentă în cadrul parchetelor. Spre deosebire de sistemul din cadrul Instanțelor unde toate aplicațiile și nodurile vor face parte dintr-un sistem comun, în cadrul parchetelor vor exista trei implementări distincte și complet separate: o implementare centralizată distinctă pentru PICCJ și parchetele subordonate, o implementare pentru DNA și structurile subordonate și o implementare pentru DIICOT și structurile subordonate. Aceste detalii sunt prezentate în diagramele de instalare (deployment). În celelalte privințe, aplicațiile sunt similare din punct de vedere al arhitecturii conceptuale, astfel în cele ce urmează sunt detaliate doar acele componente care diferă față de sistemul Instanțelor.
ECRIS CDMS Parchete este aplicația principală folosită de parchetele din România. Aplicația gestionează dosarele penale și lucrările cu specific judiciar. Utilizatorii aplicației sunt procurorii, grefierii, registratorii șamd.
În prezent aplicația se află la versiunea 3 fiind instalată local în fiecare parchet subordonat PICCJ, în timp ce DIICOT folosește o instalare centralizată, iar DNA nu folosește versiunea curentă (această instituție folosind o aplicație distinctă). O descriere a funcționalităților acestei aplicații precum și diagramele bazelor de date se regăsesc în Documentația AS-IS Parchete (livrabilul 1.3).
În noul sistem, aplicația ECRIS Parchete va fi **integral rescrisă** și va fi folosită de către cele trei structuri principale (PICCJ, DIICOT și DNA). Noua versiune 5 va include toate funcționalitățile anterioare care vor fi îmbunătățite. De asemenea la data lansării în producție, conținutul bazelor de date din aplicația curentă va trebui migrat în noua aplicație, inclusiv datele din aplicația distinctă utilizată de DNA
O funcționalitate nouă majoră a noii aplicații este dosarul electronic care va permite parchetelor o gestiune integral electronică a tuturor elementelor care compun un dosar. De asemenea aplicația ECRIS parchete va fi integrată cu aplicația ECRIS Portal Parchete și va permite ca orice interacțiune cu parchetele să se deruleze integral online.

Un alt aspect important de care furnizorul trebuie să țină cont este integrarea dintre PICCJ și Poliție. Această integrare este foarte importantă, având în vedere că cca 97% din dosarele penale sunt dosare aflate în supravegherea parchetelor, respectiv dosare unde este necesară colaborarea dintre polițiști și procurori și integrarea sistemelor Poliției și Procuraturii. Cerinte tehnice ale aplicatiei ECRIS Parchete Diagrama de instalare Ecris Parchete

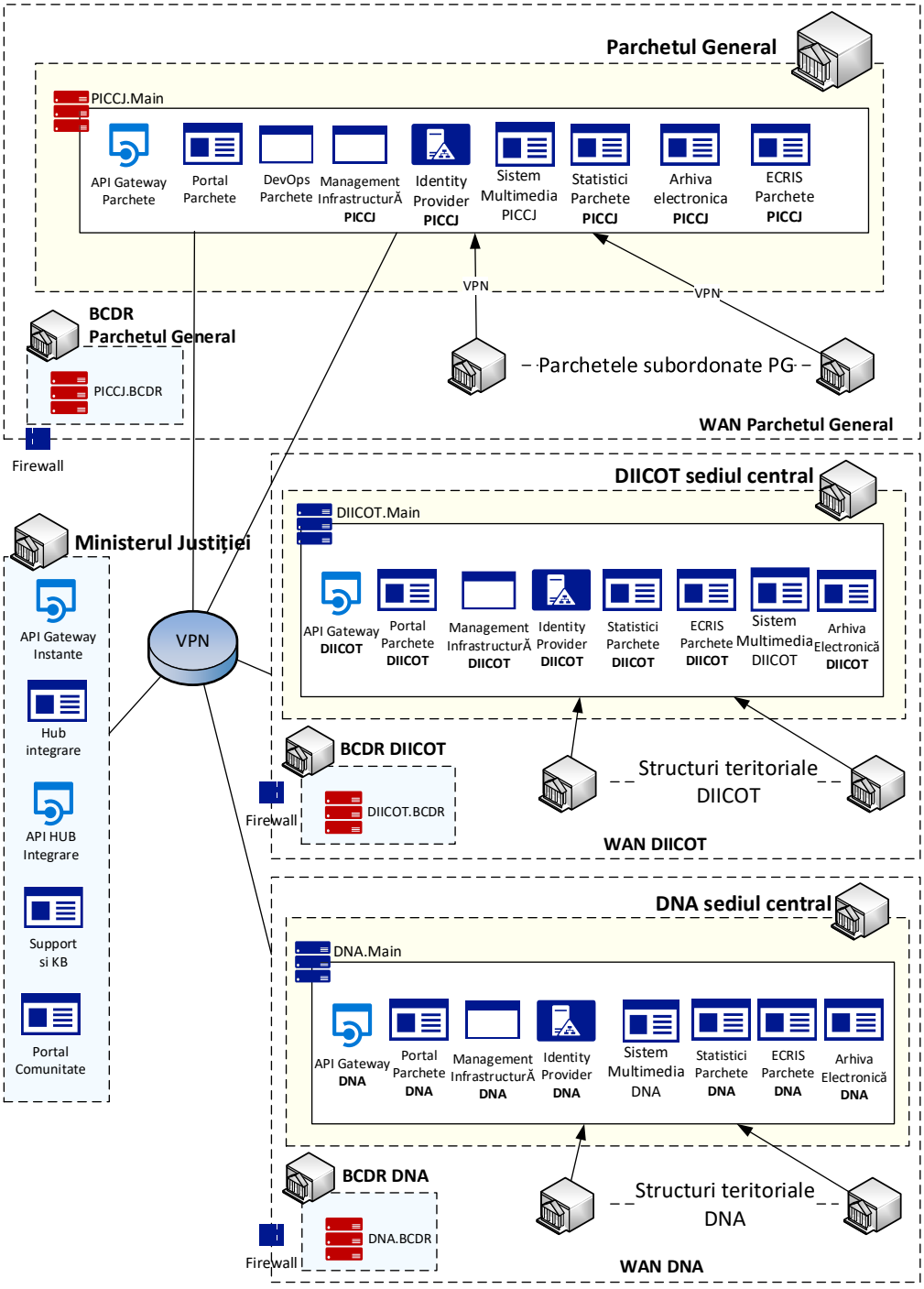


Figura 2 - Diagramă instalare parchete

În cadrul parchetelor vor exista trei instalări distincte și complet izolate. O instalare centralizată pentru PICCJ și structurile subordonate, o instalare centralizată pentru DIICOT și o instalare centralizată pentru DNA.

Cele trei instalări ale parchetelor sunt instalări centralizate care vor deservi și structurile subordonate.

Toate parchetele vor avea de asemenea acces la sistemele comune, respectiv:

- API Gateway Instanțe (pentru integrarea cu sistemul ECRIS Instanțe)
- HUB Integrare și API-ul Hub-ului de integrare
- Sistemul de suport și KB
- Portalul de comunitate

În cele ce urmează sunt descrise instalările din cadrul celor trei parchete. Structura celor trei instalări este complet identică, diferă doar echipamentele hardware care sunt dimensionate în funcție de dimensiunea fiecărei instituții. Descrierea echipamentelor hardware pentru fiecare parchet este detaliata în capitolul Arhitectură Fizică.

Parchetul General

Nodul principal instalat la parchetul general va găzdui aplicația ECRIS Parchete, Arhiva electronică pentru parchetul general și sistemul de identitate. Acest nod va fi accesat de utilizatorii din parchetul general, precum și de utilizatorii din parchetele subordonate PICCJ.

Nodul portal parchete va găzdui portalul parchetului general și API Gateway-ul aferent.

Nodul DevOps va găzdui sistemele necesare pentru DevOps (mediile de dezvoltare, testare, acceptanta, configurare etc.).

Nodul BCDR va găzdui echipamentele și aplicațiile care vor asigura continuitatea și recuperarea în caz de dezastru pentru sistemele instalate în cadrul PICCJ.

DNA și DIICOT

Instalările din cadrul DNA și DIICOT vor fi identice instalării de la PICCJ.

4.4.1 Arhitectura software ECRIS Parchete și Portal Parchete

Ca şi în cazul Instanțelor de judecată, aplicația ECRIS Parchete va fi instalată centralizat, un singur nod multi-tenant. Vor exista astfel trei instalări distincte:

- instalare centralizată care va deservi Parchetul de pe lângă Înalta Curte de Casație și Justiție și parchetele subordonate.
- instalare centralizată care va deservi Direcția Națională Anticorupție.
- instalare centralizată care va deservi Direcția de Investigare a Infracțiunilor de Criminalitate Organizată și Terorism.

Este important de subliniat că cele trei instalări ale parchetelor vor fi complet separate. Diagrama prezintă instalarea care va deservi PÎCCJ. Instalările pentru DNA și DIICOT sunt identice, cu excepția echipamentelor hardware care vor fi diferite în funcție de necesitățile fiecărei instituții.

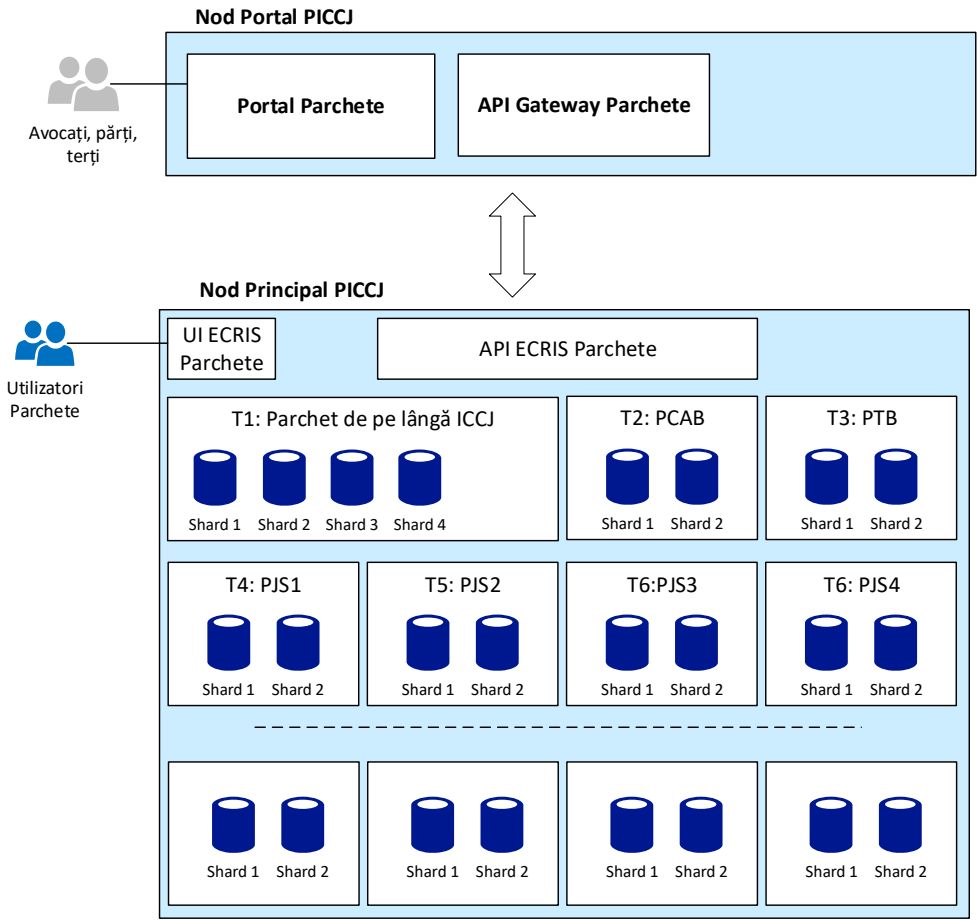


Figure 3 - Instalare PICCJ

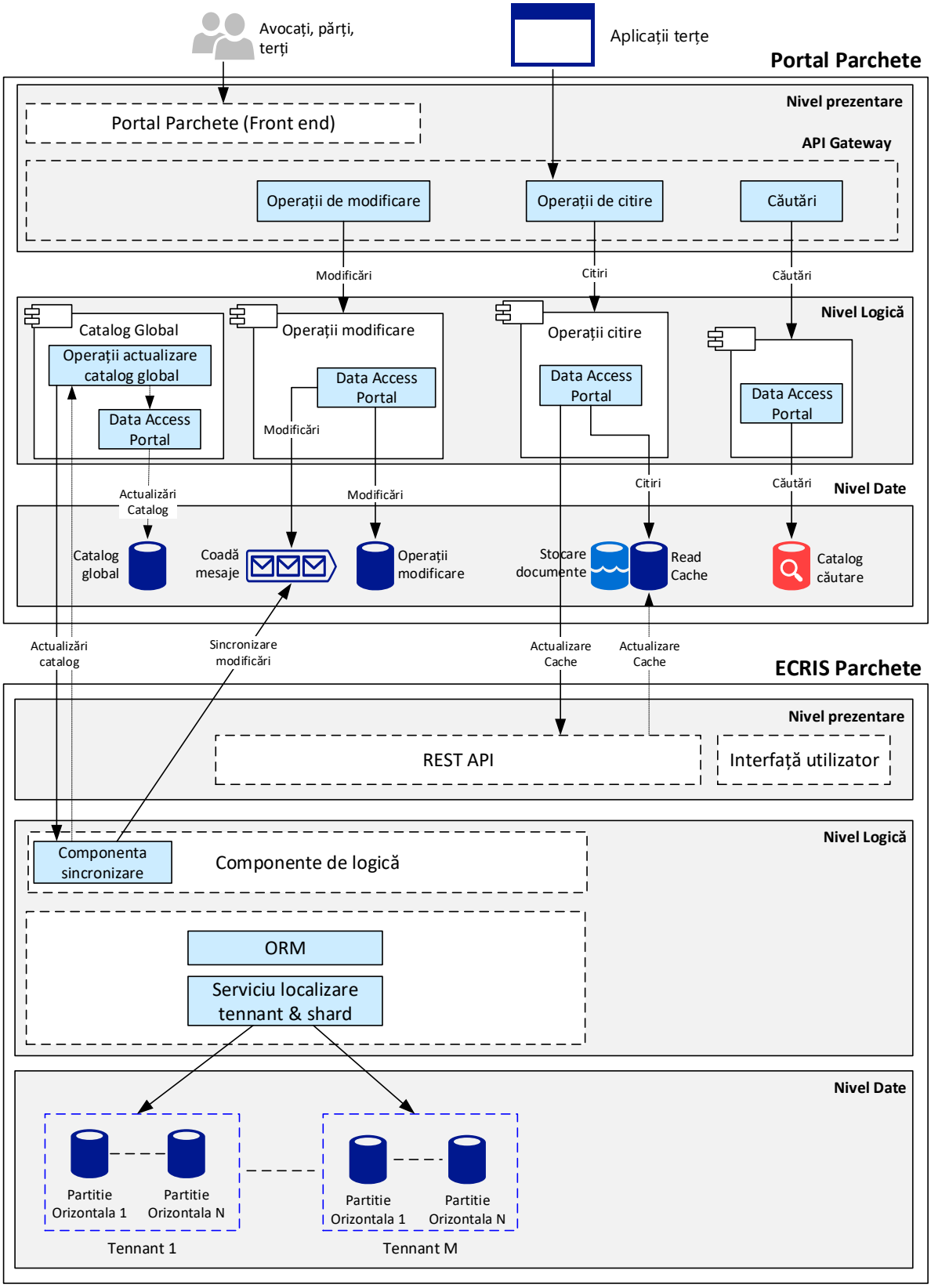


Figure 4 - Integrarea dintre ECRIS Parchete și Portal Parchete

Arhitectura ECRIS Parchete este similară ECRIS Instanțe. De asemenea arhitectura Portalului Parchetelor este similară Portalului Instanțelor. Integrarea dintre portalul parchetelor va funcționa

similar celei dintre ECRIS Instanțe și Portal Instanțe. Pentru a evita redundanțele, conceptele arhitecturale nu vor fi duplicate în cazul Parchetelor.

4.4.1.1 Informații volumetrice

În tabelul de mai jos sunt sintetizate câteva informații relevante pentru o privire de ansamblu.

Parametru	Valoare
Parametri generali	
Dimensiune stocare / pagina document (MB)	**0.125**
PICCJ	
Utilizatori interni (total angajați din schema de personal)	**4,469**
Nr de request-uri externe / zi. Estimare bazată pe traficul actual al portalului Instanțelor împărtit la 3 (având în vedere ca numărul de cauze penale este de aproximativ o treime)	**1,000,000**
Medie de dosare noi în urmărire proprie / an	**29,305**
Medie dosare în urmărire proprie soluționate / an	**22,007**
Medie de dosare noi în supraveghere /an	**615,755**
Medie dosare noi în supraveghere solutionate/an	**534,126**
Medie de lucrări / an	**1,407,106**
Medie lucrări soluționate / an	**1,344,360**
DNA	
Utilizatori interni (total angajați din schema de personal)	**316**
Nr de request-uri externe / zi (portal). 10% din traficul PICCJ	**100,000**
Medie de dosare noi în urmarire proprie / an	**5,143**
Medie dosare în urmarire proprie solutionate / an	**3,226**
Medie de lucrari de solutionat / an	**43,334**
DIICOT	
Utilizatori interni (total angajati din schema de personal)	**940**
Nr de request-uri externe / zi (portal). 20% din traficul PICCJ	**200,000**
Medie de dosare noi în urmarire proprie / an	**9,666**
Medie dosare în urmarire proprie solutionate / an	**8,594**
Medie de lucrari de solutionat / an	**99,007**

4.4.2 Documentatie tehnica AS-IS

Documentația tehnică AS-IS referitoare la ECRIS IV Parchete este descrisă în cadrul livrabilelor:

- 1.3 Documentatie AS-IS\Parchete\L1.3 ASIS Parchete - Aplicatie
- 1.3 Documentatie AS-IS\Parchete\L1.3 ASIS Parchete - Baza de date
- 1.3 Documentatie AS-IS\Parchete\L1.3 ASIS Parchete – Diagrame baza de date
- 1.3 Documentatie AS-IS\Parchete\Prosecutors db documentation.chm
- 1.3 Documentatie AS-IS\DNA\Descriere aplicatii DNA
- 1.3 Documentatie AS-IS\SAE\EAS-Specifications 1.6
- 1.3 Documentatie AS-IS\SAE\Histore DB.chm
- 1.3 Documentatie AS-IS\SAE\Manual administrare HISTORE
- 1.3 Documentatie AS-IS\SAE\Manual utilizare HISTORE
- 1.3 Documentatie AS-IS\SAE\Tech spec caiet de sarcini

4.4.3 Cerinte funcționale specifice ale aplicației ECRIS Parchete

Desi aplicația ECRIS Parchete va fi instalată pe 3 instanțe diferite (PICCJ, DNA, DIICOT), funcționalitățile acestora vor fi comune. În cadrul analizei detalitate se va stabili modul în care eventualele diferențe funcționale vor fi implementate astfel încât versiunea funcțională a aplicației să fie una comună atât la momentul implementării cât și în versiunile urmatoare.

4.4.3.1 Elemente de context, cerinte de business si functionalitati

Informațiile referitoare la Elemente de context, cerințe de business și funcționalități ECRIS V Parchete care trebuie acoperitee sunt descrise în cadrul livrabilelor:

- L1.2-Parchete-diagrama de context
- L1.2-Parchete-diagrame procese de business
- L1.2-Parchete-Elemente de context, cerințe de business și functionalități cheie ale sistemului
- L1.3-Parchete-Entitati de business

4.4.3.2 Specificatiile functionale ale ECRIS V Parchete

Cerințele funcționale pe care aplicația ECRIS V Parchete trebuie sa le acopere sunt descrise în cadrul livrabilelor:

- L2-Parchete-Portal-Specificații funcționale
- L2-Parchete-Functionalități-Specificații funcționale
- L2-Parchete-Anexe documente
- L2-Parchete-Integrari
- L2-Parchete-Machete de ecrane
- L2-Model de date detaliat
- L2-Parchete-Rapoarte

4.4.4. Dosarul electronic ECRIS Parchete

O funcționalitate majoră a noii aplicații este dosarul electronic care va permite Parchetelor o gestiune integral electronică a documentelor din dosare. De asemenea aplicația ECRIS Parchete va fi integrată cu aplicația ECRIS Portal Parchete și va permite ca orice interacțiune cu Instanțele să se deruleze integral online.
Cerințele tehnice pe care Dosarul electronic ECRIS V trebuie sa le îndeplinească sunt descrise in cadrul Componentei **Stocarea si accesul la documentele electronice.**

4.4.4.1 Informații volumetrice

In tabelul de mai jos sunt sintetizate câteva informații relevante pentru o privire de ansamblu.

Parametru	Valoare
PICCJ	
Utilizatori interni (total angajați din schema de personal)	**4,469**
Nr de request-uri externe / zi. Estimare bazată pe traficul actual al portalului Instanțelor împărtit la 3 (având în vedere ca numărul de cauze penale este de aproximativ o treime)	**1,000,000**

Medie de dosare noi în urmărire proprie / an	**29,305**
Medie dosare în urmărire proprie soluționate / an	**22,007**
Medie de dosare noi în supraveghere /an	**615,755**
Medie dosare noi în supraveghere solutionate/an	**534,126**
Medie de lucrări / an	**1,407,106**
Medie lucrări soluționate / an	**1,344,360**
DNA	
Utilizatori interni (total angajați din schema de personal)	**316**
Nr de request-uri externe / zi (portal). 10% din traficul PICCJ	**100,000**
Medie de dosare noi în urmarire proprie / an	**5,143**
Medie dosare în urmarire proprie solutionate / an	**3,226**
Medie de lucrari de solutionat / an	**43,334**
DIICOT	
Utilizatori interni (total angajati din schema de personal)	**940**
Nr de request-uri externe / zi (portal). 20% din traficul PICCJ	**200,000**
Medie de dosare noi în urmarire proprie / an	**9,666**
Medie dosare în urmarire proprie solutionate / an	**8,594**
Medie de lucrari de solutionat / an	**99,007**

4.4.4.2 Sistem de stocare si redare Video / Multimedia

Sistemul va permite stocarea de conținut video și audio în dosarul electronic de parchet. Acest sistem va asigura persistența înregistrărilor audio și video și integrarea cu aplicația ECRIS Parchete, ECRIS Instanțe și sistemul video de la Instanțe. În cadrul ECRIS Parchete, înregistrările video și audio vor fi parte din dosarul electronic. Sistemul trebuie să ofere posibilitatea de streaming video și audio, astfel încât un utilizator al aplicației ECRIS Parchete (procuror/grefier) să poată accesa foarte ușor o înregistrare video sau audio, fără a fi nevoit să descarce integral fișierul pe calculatorul propriu.
Sistemul trebuie să asigure și transformarea (encoding) fișierelor multimedia într-un format potrivit pentru streaming multimedia (ex: H.264 sau H.265 preferabil datorită compresiei mai bune). Standardul de compresie va fi stabilit în perioada de implementare.
IMPORTANT: din motive legale, în cazul fișierelor video și audio ce vor fi convertite la un standard comun, sistemul va păstra și originalul. De asemenea sistemul trebuie să permită semnarea și marcarea temporară a conținutului pentru a se împiedica alterarea acestora.
Cerintele tehnice pe care Sistemul de stocare si redare Video / Multimedia trebuie sa le indeplinească sunt descriese în cadrul Componentei **Stocarea și accesul la documentele electronice.**
Pentru parchete (PICCJ și parchete nespecializate – cerințele implică și integrarea cu SMIA (proiectul separat -Sistem de Management Integrat al audierilor) – menționată în L2 - Parchete – Integrări.

4.4.5 Nomenclatoare ECRIS Parchete

O componentă importantă a functionalităților ECRIS Parchete o reprezintă Nomenclatoarele specifice. Aceste nomenclatoare sunt descrise în cadrul capitolului/documentului(lor) L2 - Parchete - Model de date detaliat (capitol 2.1.2.2 Nomenclatoare parchete).
De aemenea, există o serie de nomenclatoare comune între ECRIS Instanțe și Ecris Parchete care trebuie implementante și administrate în mod unitar. Aceste nomenclatoare sunt descrise în cadrul livrabilul/livrabilele L2 - Parchete - Model de date detaliat (capitol 2.1.2.1 Nomenclatoare comune).

4.4.6 Rapoarte ECRIS Parchete

Pentru raportare se vor folosi baze de date distincte, astfel încât interogările de raportare să nu afecteze performanța aplicațiilor principale. În funcțiile de cerințele de raportare ale aplicației, bazele de raportare pot fi replici OLTP peste care opțional se pot construi baze de date OLAP.
Implementarea de baze de date OLAP este recomandată cel puțin pentru aplicațiile de Statistici, ECRIS Instanțe și ECRIS Parchete.
Rapoartele aferente ECRIS Parchete care vor fi disponibile parchetelor sunt impărțite în două categorii:

4.4.6.1 Rapoarte Operationale Parchete

Rapoartele Operationale **Parchete** sunt rapoarte predefinite care vor putea rula direct pe baza de date ECRIS Parchete. Aplicația va oferi un modul de raportare comun pentru toate Parchetele. Accesul la rapoarte este limitat printr-un sistem de roluri și permisiuni.
În functie de informațiile conținute de acestea, unele dintre acestea nu vor pute fi rulate decat de persoane cu drept de administrator pentru instanța/instanțele respective.
Detaliile funcționale ale acestor rapoarte sunt descrise în cadrul livrabilului L2-Parchete-Rapoarte

4.4.6.2 Rapoarte Statistice Parchete

Statistici Parchete
Aplicația oferă un modul de raportare comun pentru fiecare structură de parchet, fiind bazat pe o bază de date comună care include date înregistrate în fiecare din aplicațiile ECRIS parchete. Accesul la rapoarte este limitat printr-un sistem de roluri și permisiuni. Aplicația va fi instalată distinct pentru PICCJ, DNA și DIICOT.
Modul de acces și generare a rapoartelor Statistice Parchete este descris în cadrul componentei Statistică Judiciară.
Aplicația va oferi un modul de raportare comun pentru toate instanțele Ecris Parchete. Accesul la rapoarte este limitat printr-un sistem de roluri și permisiuni.
În funcție de informatiile conținute de acestea, unele dintre acestea nu vor pute fi rulate decat de persoane cu drept de administrator pentru instanta/instantele respective.
Detaliile funcționale ale acestor rapoarte sunt descrise in cadrul livrabilului: L2 - Parchete – Rapoarte.

4.4.7 Integrari ECRIS Parchete

Integrările necesare sistemului ECRIS sunt enumerate în documentul „2.2.1.B – Integrări între sisteme” parte din livrabilul 2.2.1 – Cerințe non-funcționale. Prin integrare înțelegem conectarea directă, la nivel tehnic, dintre două sisteme informatice cu scopul de a schimba informații relevante pentru ambele sisteme.
Integrările dintre aplicațiile sistemului ECRIS se împart în două categorii:

- Integrările dintre aplicațiile sistemului ECRIS.
- Integrări dintre aplicații ale sistemului ECRIS și aplicații externe.

Prin aplicație externă înțelegem orice aplicație ce nu face parte din scopul sistemului ECRIS, inclusiv aplicații operate de instituții din sistemul de justiție.
Toate integrările necesare sunt enumerate în documentul L2.2.1.B – Integrari intre sisteme.xlsx (sublivrabil al livrabilului 2.2.1 – Cerinte non-functionale).

4.4.7.1 Integrari ECRIS Parchete cu componentele interne ECRIS 5 (inclusiv Portaluri)

4.4.7.1.1 API Gateway Parchete

Componenta API gateway pentru parchete este similară componentei API Gateway Instanțe.

4.4.7.1.2 Integrarea ECRIS Parchete cu ECRIS Instanțe

Detaliile funcționale ale acestei integrari sunt descrise în cadrul livrabilului L2 - Parchete - Integrări

4.4.7.1.3 Integrarea ECRIS Parchete cu Portal Parchete

Portalul parchetelor va utiliza funcțiile oferite de API gateway, respectiv portalul va expune funcționalitatea oferită de componenta API gateway sub forma unei interfețe utilizator. În acest sens portalul va fi strict o interfață utilizator (front-end) și nu va implementa logica proprie, toate funcțiile necesare fiind implementate la nivelul API Gateway.
Cerințele de integrare specifice sunt detaliate in livrabilul L2 - Parchete - Portal - Specificații funcționale

4.4.7.1.4 Integrarea ECRIS Parchete cu Inspectia Judiciara

Cerințele de integrare specifice sunt detaliate in livrabilul L2 - IJ - Specificații funcționale - faza II Subcapitolul 2.3

4.4.7.1.5 Integrare ECRIS Parchete cu DNP (Probatiune)

Cerințele de integrare specifice sunt detaliate în livrabilul L2 - Parchete - Integrări

4.4.7.2 Integrari cu componente externe ECRIS 5

4.4.7.2.1 API Gateway parchete

Componenta API gateway pentru parchete este similară componentei API Gateway Instanțe.

4.4.7.2.2 Integrare ECRIS Parchete cu ANABI

Componenta asigură interfațarea sistemului implementat de ANABI, de evidență a bunurilor sechestrate, confiscate și valorificate în cadrul procesului penal cu aplicațiile ECRIS Parchete și ECRIS Instanțe. Scopul interfațării este de a comunica date despre ordonanțele procurorilor sau hotărârile judecătorești privind bunurile indisponibilizate, precum și detalii referitoare la administrarea și valorificarea acestora. Din punct de vedere tehnic ECRIS ANABI nu este o aplicație distinctă ci o componentă care va asigura integrarea dintre celelalte aplicații ale sistemului ECRIS cu sistemul ANABI care nu face parte din scopul dezvoltării.
Detalierea cerințelor de integrare se regăsesc în livrabilului L2 - Parchete – Integrări

4.4.8 Arhiva Electronica Parchete

Arhiva electronică a parchetelor este similară cu arhiva electronică disponibilă în cadrul Instanțelor. Arhivarea electronica a dosarelor din instante se va efectua in două etape:

4.4.8.1 Arhivarea Logica Parchete:

În cadrul sistemului ECRIS vor fi prevăzute două tipuri de arhivare: logică și permanentă. Arhivarea logică va păstra informațiile în sistemele de stocare online iar informațiile arhivate vor fi marcate logic ca fiind arhivate (flag de arhivare). Arhivarea permanentă va presupune transferarea efectivă a datelor în sisteme de arhivare dedicate cu caracteristici WORM.

IMPORTANT: pentru arhivarea logică datele vor fi păstrate în aceleași tabele și baze de date, dar vor fi marcate logic ca fiind arhivate, respectiv datele NU vor fi transferate în alte tabele sau baze de date dedicate arhivei logice. Transferul datelor arhivate logic în cadrul aceleiași baze de date generează în timp complexitate nenecesară care nu poate fi ușor controlată și din acest motiv această abordare NU este recomandată. Această abordare a fost folosită în ECRIS 4 și versiunile anterioare unde și-a dovedit ineficacitatea. Astfel datele arhivate logic vor fi păstrate în aceleași tabele cu datele nearhivate, iar filtrarea se va realiza prin intermediul unor structuri de tip view (recomandat) sau la nivel de logică de aplicație. Pentru aplicațiile care folosesc sharding, este recomandat ca datele arhivate să fie persistate în shard-uri dedicate arhivei logice pentru a descărca bazele de date online, cu condiția ca distribuirea să facă parte din strategia normală de sharding. Altfel spus este esențial ca datele arhivate logic să NU primească un tratament separat în logica aplicației (în afara eventualei filtrări logice), respectiv o interogare (query) care cuprinde atât date nearhivate cât și date arhivate logic, nu trebuie să fie cu nimic diferită față de o interogare care cuprinde doar date nearhivate sau doar date arhivate. În eventualitatea în care datele arhivate sunt stocate în shard-uri separate, un astfel de query va fi rezolvat prin mecanismul general de interogare multi-shard, în mod transparent pentru componentele de logică ale aplicației.
Detaliile tehnice generale pentru aceste funcționalități se regăsesc descrise amănunțit în cadrul componentei Arhiva Electronica.

4.4.8.2 Arhivarea Permanenta Parchete:

Aplicația de arhivă electronică va asigura arhivarea permanentă a informațiilor din aplicațiile sistemului ECRIS cu excepția aplicațiilor dedicate parchetelor care vor beneficia de o componentă de arhivare dedicată. Informațiile arhivate vor fi stocate pe echipamente specializate tip WORM.
Detaliile tehnice generale pentru aceste funcționalități se regăsesc descrise amănunțit în cadrul componentei Arhiva Electronica.

4.4.9 Cerinte de Securitate ECRIS Parchete

Cerințele tehnice generale sunt detaliate în cadrul componentei Cerinte de Securitate
Cerințele de Securitate sunt împărțite în trei categorii:

4.4.9.1 Securitatea stocarii si auditarii datelor/documentelor

Cerințele tehnice generale sunt detaliate în cadrul componentei Cerinte de Securitate
Cerințele specifice pentru ECRIS Parchete sunt detaliate in cadrul livrabilului 3.1. Specificatii securitate

4.4.9.2 Securitatea accesului la date/documente

Sistem de identitate parchete (Identity Provider) Componenta este similară celei disponibile în cadrul Instanțelor.

În cazul aplicatiei ECRIS Parchete trebuie avut in vedere ca deși din punct de vedere tehnic și funcțional aceasta va fi o solutie unică, vor exista trei instanțe de aplicatie și DB instalate separat cu propriul sistem de administrare, inclusive cel de identitate.
Cerințele specifice:
Pentru autentificarea utilizatorilor și aplicațiilor în cadrul ECRIS Parchete este necesară implementarea unui **sistem de identitate (Identity Provider).** Acest sistem va fi un sistem de tip Single Sign-On pentru toate aplicațiile dezvoltate în cadrul sistemului ECRIS. Sistemul va permite ca utilizatorii să poată folosi un singur cont de utilizator pentru a accesa orice aplicație din sistemul ECRIS, în funcție de drepturile pe care le au.
Acest sistem trebuie să implementeze cel puțin un standard deschis de autentificare (spre exemplu OAuth 2.0) astfel încât integrarea cu aplicațiile dezvoltate să fie ușor de realizat. Toate aplicațiile din sistemul ECRIS vor folosi serviciile sistemului de identitate pentru autentificarea utilizatorilor și nu vor implementa propriile mecanisme de autentificare. Autorizarea accesului la resurse va fi implementată la nivelul fiecărei aplicații și API.
Sistemul trebuie să ofere facilități clasice de înregistrare, resetare a parolei etc. precum și posibilitatea autentificării de tip multi-factor (ex: parolă și SMS / email). Sistemul trebuie să permită posibilitatea de a asocia un certificat digital contului unui utilizator (respectiv asocierea cheii publice cu un cont). Această funcție este necesară pentru asigurarea funcționalității de validare a semnăturilor electronice. De asemenea pentru utilizatorii care dețin un certificat digital, acesta ar trebui să poată fi folosit inclusiv pentru autentificare.
Sistemul trebuie să ofere funcționalități de validare a identității. Această cerință este necesară pentru a valida identitatea terților care vor interacționa online prin intermediul portalului. Procesul de validare a identității este descris în cerințele funcționale.

4.4.9.3 Securitatea transferului datelor/documentelor

Cerințele tehnice generale sunt detaliate în cadrul componentei Cerințe de Securitate

4.4.10 Cerințe non-functionale legate de ECRIS Parchete

Cerințele non-funcționale generale sistemului ECRIS sunt detaliate în cadrul componentei Cerințe non-funcționale.

4.4.11 Administrare ECRIS Parchete

Cerințele Tehnice generale se regăsesc în cadrul Componentei Administrare Sistem Ecris.
Componentele principale ale acestui modul sunt urmatoarele:

4.4.11.1 Atribuire/Definire Roluri Utilizator si drepturi specifice de acces ECRIS Parchete

În cazul aplicației ECRIS Parchete trebuie avut în vedere că deși din punct de vedere tehnic și funcțional aceasta va fi o soluție unică, vor exista trei instanțe de aplicație și DB instalate separat cu propriul sistem de administrare, inclusive cel de identitate.
Cerințele tehnice sau functionale specifice ECRIS Parchete sunt detaliate in cadrul livrabilului L2 - Parchete - Functionalități - Specificații funcționale (capitolul 2.10 Administrare)

4.4.11.2 Administrare Nomenclatoare Specifice ECRIS Parchete

În cazul aplicației ECRIS Parchete trebuie avut în vedere că deși din punct de vedere tehnic și funcțional aceasta va fi o soluție unică, vor exista trei instante de aplicatie și DB instalate separat cu propriul sistem de administrare, inclusive cel de identitate.
Cerințele tehnice sau funcționale specifice ECRIS Parchete sunt detaliate în cadrul livrabilului /livrabilelor:

- L2 - Parchete - Model de date detaliat (capitol 2.1.2.2 Nomenclatoare parchete)..
- L2 - Parchete - Functionalitati - Specificatii functionale (capitolul 2.10 Administrare)

4.4.11.3 Adiministrare si Generare Rapoarte (operationale sau statistice) ECRIS Parchete

Cerințele tehnice sau funcționale specifice ECRIS Parchete sunt detaliate in cadrul livrabilului L2 - Parchete - Rapoarte

4.4.11.4 Alte Cerinte de Administrare specifice ECRIS Parchete

Cerințele tehnice sau funcționale specifice ECRIS Parchete sunt detaliate în cadrul livrabilului L2 - Parchete - Funcționalități - Specificații funcționale (Capitolul 2.10 Administrare)

4.4.12 Tranzitie ECRIS Parchete

Strategia generală de tranzite la Sistemul ECRIS V este descrisă în cadrul componentei Tranziție.
Elementele specifice ECRIS Parchete:

4.4.12.1 Migrare Date ECRIS Parchete

Strategia generala este descrisa in cadrul componentei Tranzitie

Cerințe specifice:

4.4.12.1.1 Situatia Actuala

4.4.12.1.1.1PICCJ și DIICOT

Pentru evidența dosarelor, atât în cadrul Parchetului de pe lângă Înalta Curte de Casație și Justiție (PICCJ) cât și în cadrul Direcției de Investigare a Infracțiunilor de Criminalitate Organizată și Terorism (DIICOT), este folosită aplicația ECRIS Prosecutors. Această aplicație este instalată centralizat pentru DIICOT. Pentru PICCJ această aplicație este instalată pe un server local în cadrul fiecarui parchet subordonat.
Pentru evidența documentelor electronice doar PICCJ foloseste aplicație SAE.
Documentația pentru aplicația ECRIS CDMS Prossecutors se găsește în cadrul livrabilului 1.3 Documentatie AS-IS si cuprinde:
- Documentatie AS-IS high-level realizata in cadrul proiectului SIPOCA55
- Documentatie detaliata a bazelor de date folosite de aplicatie realizată în cadrul proiectului SIPOCA55
- Documentația bazelor de date in format CHM furnizată de beneficiar

4.4.12.1.1.2DNA

Pentru evidența dosarelor penale DNA și pentru evidența cauzelor aflate pe rolul instanțelor, DNA folosește două aplicații dezvoltate intern de specialiștii IT ai acestor instituții. O descriere a acestor aplicații și a bazelor de date folosite se găsește în livrabilul 1.3 Documentatie AS-IS. Având în vedere caracterul sensibil al acestor aplicații, o diagramă completă a bazelor de date nu este anexată caietului de sarcini, însă informațiile furnizate în documentul de descriere sunt suficiente pentru a

înțelege complexitatea acestor baze de date și pentru a estima efortul necesar migrării datelor. O diagramă detaliată a bazelor de date și detalii tehnice suplimentare vor fi furnizate de DNA furnizorului câștigător, ulterior încheierii contractului de implementare.
Și în cadrul DNA este utilizată aplicația SAE, descrisă mai sus, pentru evidența documentelor electronice.

4.4.12.2 Scop Migrare ECRIS Parchete

4.4.12.2.1 PICCJ

Pentru PICCJ aplicația ECRIS curentă este instalată pe un server local în cadrul fiecarui parchet subordonat.
Instrumentele de migrare pentru PICCJ vor migra datele din sistemul ECRIS și sistemul SAE în noua bază de date. Migrarea datelor PICCJ se va finaliza cel mai târziu cu 3 luni înainte de finalizarea proiectului.
Migrarea datelor din PICCJ este similară cu migrarea datelor din instanțe. Numărul total de parchete este 240, dintre care:

- 1 – PICCJ
- 15 – Parchete de pe lângă Curți de Apel
- 42 – Parchete de pe lângă Tribunale
- 1 – Parchet de pe lângă Tribunal specializat
- 176 – Parchete de pe lângă Judecătorii
- 4 – Parchete de pe lângă Tribunalele militare
- 1 – Parchet de pe lângă Curtea Militară de apel

Pentru PICCJ si parchetele subordonate se va aplica strategia de migrare treptată, descrisă pentru instanțe, grupurile fiind formate din parchetele de pe lângă curțile de apel împreună cu parchetele de pe lângă tribunalele și parchetele de pe lângă judecătoriile arondate. De semenea primul grup de parchete va conține și parchetul de pe Înalta Curte de Casație și Justiție.

4.4.12.2.2 DIICOT

DIICOT folosește o instalare centralizată a versiunii curente a aplicației ECRIS.
Instrumentele de migrare pentru DIICOT vor migra datele din sistemul ECRIS și sistemul SAE în noua baza de date. Migrarea datelor DIICOT se va finaliza cel mai târziu cu 3 luni înainte de finalizarea proiectului.

4.4.12.2.3 DNA

DNA folosește o instalare centralizată a aplicațiilor, astfel din punct de vedere operațional migrarea acestor date este mai simplă față de instanțe. Instrumentele de migrare pentru DNA vor migra simultan datele din cele două aplicații folosite de DNA și sistemul SAE în noua baza de date. Migrarea datelor DNA se va finaliza cel mai târziu cu 3 luni înainte de finalizarea proiectului.În cadrul aplicației aflate în producție utilizatorii au procedat la introducerea datelor folosind caractere cu diacritice specifice tastaturilor Română Tradițional (Legacy) și Română Standard, aspect de care trebuie ținut cont la migrarea datelor din bazele actuale, în vederea afișării corecte a datelor. Din perspectiva filtrelor, căutarea datelor trebuie să fie “accent-insensitive” și “case-insensitive”, pentru a determina apariția tuturor rezultatelor posibile.

4.4.12.3 Acceptanță Migrare

Acceptanța migrărilor se va realiza la finalul proiectului, ca parte din procesul general de acceptanță. Criteriile de acceptanță a activității de migrarea vor urmări migrarea integrală a datelor din toate bazele de date avute în scop în noile baze de date ECRIS, respectiv:

- Toate bazele de date ECRIS Prosecutors utilizată de PICCJ și instituțile subordonate.
- Toate bazele de date SAE utilzată de PICCJ și instituțile subordonate.
- Baza de date ECRIS Prosecutors utilizată de DIICOT
- Baza date ale aplicațiilor utilizate de către DNA
- Baza de date SAE utilzată de DNA

4.4.13 Intruire ECRIS Parchete

Strategia generală este descrisă în cadrul componentei Tranziție

4.4.14 Roll-out ECRIS Parchete

Strategia generală este descrisă în cadrul componentei Tranziție

4.5 Nomenclatoare comune ECRIS Instante si Parchete

4.5.1 Cerinte tehnice specifice

Cerințele tehnice specifice Nomenclatoarelor comune vor fi detaliate în etapa de analiză detaliată.

4.5.2 Administrare Nomenclatore commune

ECRIS Admin
Aplicația ECRIS Admin cumulează funcționalități de administrare a sistemelor ECRIS, spre exemplu administrarea nomenclatoarelor globale.

5. Cerinte de Securitate

Securitate și protecția datelor personale
În mod evident, securitatea informațiilor stocate în sistemul ECRIS este esențială. În acest sens accesul la toate informațiile sistemului trebuie securizat, iar permisiunile vor fi acordate explicit, nu implicit. De asemenea trebuie ținut cont că anumite informații stocate în sistem trebuie anonimizate (ex: datele personale ale martorilor protejați, datele personale ale minorilor etc). Noul sistem ECRIS, prin sistemele de portal, va avea o componenta de interacțiune cu publicul. În acest sens este importantă respectarea prevederilor GDPR.
Pentru implementarea securității se va aplica principiul celui mai mic privilegiu (POLP), respectiv unui utilizator sau sistem i se vor acorda doar drepturile strict necesare pentru îndeplinirea unei acțiuni. Mecanismele de securitate vor fi implementate la fiecare nivel al aplicațiilor.
Pentru implementarea mecanismelor de securitate (ex: autentificare) se vor utiliza standarde deschise și componente existente, fiind excluse implementările personalizate (custom).
Flexibilitatea mecanismelor de autorizarea este de asemenea importantă. Pentru a oferi flexibilitatea în privința configurărilor de securitate se va folosi un sistem bazat pe permisiuni tip CBAC (claim based access control) și se va evita folosirea unui sistem tip RBAC (role based access control). Pentru implementarea autorizării se vor folosi componente comune și reutilizabile cu scopul de a crea un sistem foarte robust de definire a drepturilor de acces la resurse (informații, documente, operații

etc.). La nivel de baze de date, se vor putea defini permisiuni atât la nivel de coloane (atribute) cat și la nivel de înregistrări (obiecte).

5.1 Cerințe Generale de Securitate

Arhitectura ECRIS trebuie să respecte reglementările legale privind GDPR ca și principiu de bază. În acest sens, securitatea datelor prelucrate de sistemul informatic, inclusiv din punct de vedere al comunicațiilor, dintre entitățile participante în sistem trebuie să fie conformă normelor legale.
ECRIS trebuie să asigure mecanisme de protecție împotriva încercărilor deliberate sau accidentale de acces neautorizat la datele pe care acesta le gestionează. Soluția de securitate trebuie să asigure securitatea și confidențialitatea datelor cu caracter personal ale cetățenilor existente în bazele de date. Astfel, utilizatorii vor putea accesa numai acele secțiuni și acel conținut care le sunt permise prin apartenența la un profil sau la o machetă de securitate.
Soluția de securitate va fi configurată astfel:
• să nu permită persoanelor neautorizate să modifice sau să altereze informațiile din sistem;
• să nu permită persoanelor neautorizate să acceseze sistemul;
• să asigure integritatea și autenticitatea datelor și să permită identificarea sursei datelor inițiale și a persoanelor care au accesat sau au înregistrat aceste date în sistem;
• să asigure trasabilitatea acțiunilor utilizatorilor și operațiunilor efectuate în sistem;
• nu va exista posibilitatea de acces pentru persoanele dintr-un mediu extern la date dintr-un mediu considerat intern;
• informațiile private care se transmit vor fi criptate până la livrare, astfel să nu poată fi interceptate și utilizate;
• informațiile vor putea fi protejate integral și în permanență pentru acces neautorizat;
• grupurile de utilizatori vor putea fi setate pentru diferite niveluri de acces în sistem;
• sistemul va permite auditul complet al accesului utilizatorilor la aplicații și la baza de date prin înregistrarea orei și datei la care a fost executată fiecare tranzacție, precum și identitatea utilizatorului care a inițiat-o;
• vor exista facilități de generare parole, precum și stabilire de reguli specifice (lungime de parolă, timp de expirare parolă, numărul maxim de erori tolerate la introducerea parolei după care utilizatorul este automat blocat);
• va oferi posibilitatea de blocare facilă și selectivă a utilizatorilor;
• va asigura securitatea tuturor interfețelor sistemului informatic prevenind accesul utilizatorilor neautorizați la sistem;
• nu va permite utilizatorilor obisnuiți accesul la datele din baza de date doar prin intermediul funcțiilor incluse în sistemul informatic (ecrane dedicate);
• în caz de avarii vor exista înregistrate suficiente informații de diagnosticare pentru a ajuta la identificarea și soluționarea problemei.

Accesul la date trebuie să se facă doar prin intermediul serviciilor/interfețelor oferite de componentele informatice, pe baza drepturilor deținute de către utilizatori, accesul direct la datele din tabele nefiind permis. De asemenea, accesul trebuie să fie reglementat prin politicile de securitate aferente fiecărui tip de utilizator.
Sistemul trebuie să includă mecanisme pentru asigurarea următoarelor servicii de securitate:
• confidențialitatea, care asigură că datele sunt accesibile, vizibile sau disponibile doar utilizatorilor autorizați atât pentru datele stocate cât și pentru cele care tranzitează sistemul;
• integritatea, care asigură nealterarea datelor sau distrugerea acestora de către o acțiune neautorizată;

• disponibilitatea, asigură că resursele de informații să fie accesibile și utilizabile la cererea personalului autorizat atunci când le sunt necesare;
• autentificarea, este mecanismul prin care un utilizator demonstrează că este autorizat să utilizeze sistemul;
• nonrepudierea, este un serviciu care nu permite unui utilizator participant la introducerea, modificarea sau manipularea datelor prin sistem să decline faptul că el a fost inițiatorul unei anumite acțiuni. Semnătura digitală este o soluție tehnică utilizată frecvent pentru realizarea serviciului de nonrepudiere.

Sistemul va fi proiectat astfel încât să respecte Regulamentul (UE) 2016/679 al Parlamentului European și al Consiliului din 27 aprilie 2016 privind protecția persoanelor fizice în ceea ce priveste prelucrarea datelor cu caracter personal și privind libera circulație a acestor date și de abrogare a Directivei 95/46/CE precum și legislația națională în domeniul prelucrării datelor cu caracter personal.
Confidențialitatea este o caracteristică de bază pentru furnizarea serviciilor publice.
În cadrul implementării ECRIS se vor respecta următoarele principii:
• că urmează abordarea confidențialității prin concepție pentru a asigura securitatea modulelor și a infrastructurii lor complete;
• că respectă cerințele și obligațiile juridice privind protecția și confidențialitatea datelor recunoscând riscurile la adresa confidențialității care reies din analiza și prelucrarea avansată a datelor.

De asemenea, trebuie să asigure respectarea de către beneficiari a legislației privind protecția datelor, prin:
• Un „plan de acces la date și autorizare" care stabilește persoanele care au acces la date, datele care sunt accesibile și condițiile accesării datelor, pentru a asigura confidențialitatea. Accesul neautorizat și încălcarea normelor de securitate trebuie monitorizat, iar măsurile corespunzătoare pentru a preveni orice repetare a încălcărilor trebuie documentate și planificate;
• Utilizarea unor servicii calificate de asigurare a încrederii în conformitate cu regulamentul eIDAS pentru a asigura integritatea, autenticitatea, confidențialitatea și nerepudierea datelor.

Validarea de securitate a actualizărilor software înainte de publicare:
Sistemul trebuie să permită scanarea automată de vulnerabilități cunoscute și de bune practici de programare a versiunilor propuse spre actualizare, înainte ca acestea să fie publicate către utilizatori. Sistemul va permite blocarea publicării versiunii în cazul în care sunt identificate defecțiuni de programare sau vulnerabilități de natură să afecteze buna funcționare a sistemului.

Securizarea datelor prin criptarea dublă
Sistemul trebuie să ofere mecanisme prin care să se permită criptarea și securizarea la mai multe niveluri ale sistemului:
- Datele stocate
- Datele care circulă pe rețea
- Configurări specifice aplicației (utilizatori, parole de acces, chei de acces)
Fiecare mecanism de protecție va fi securizat prin chei și protocoale distincte. Modificarea lor nu va putea fi posibilă decât de către administratorii desemnați.
Pentru protecția datelor se vor folosi și următoarele mecanisme:
- IEEE 802.1AE Media Access Control Security (criptare a comunicației la nivel de rețea)
- Hardware Security Module (HSM) (gestiune controlată a cheilor de criptare)

Politici de securitate si audit

Sistemului ECRIS trebuie să fie implementat într-un mod securizat astfel încât să se asigure toate elementele necesare păstrării confidențialității, integrității și disponibilității datelor din dosarele administrate de acesta. Coordonarea unei implementări sigure și ulterior operării în siguranță a sistemului ECRIS se face prin intermediul politicilor, ghidurilor și procedurilor de securitate.

Beneficiarii sistemului ECRIS au deja definite o serii de politici și proceduri pentru asigurarea unui nivel de securitate corespunzător, dar acestea trebuie actualizate și îmbunătățite cu noi proceduri și politici în funcție de elementele noi incluse in sistemul ECRIS. Este responsabilitatea furnizorului să asigure alinierea politicilor și procedurilor existente cu noile reglementări sau bune practici internaționale precum și definirea unor politici noi

Politici de securitate

Pe parcursul perioadei de implementare al noului sistem ECRIS, furnizorul are obligația de a actualiza sau defini politicile de securitate ale beneficiarului astfel încât implementarea să fie aliniată la cele mai bune practici în domeniu. Aceste politici trebuie să includă cel puțin:

- gestionarea cheilor criptografice
- managementul conturilor privilegiate
- managementul vulnerabilităților și al actualizărilor
- segmentare rețea

Stabilirea de politici și proceduri pentru gestionarea cheilor criptografice din sistem. Acestea trebuie să includă, dar fără a se limita la:

- gestionarea ciclului de viață al cheilor de la generare până la revocare și înlocuire;
- specificații pentru infrastructura cu cheie publică (Public Key Infrastructure - PKI);
- definirea protocoalelor criptografice și a algoritmilor utilizați în gestiunea cheilor;
- definirea controalelor de acces în vederea generării și schimbului securizat a cheilor;
- definirea criteriilor de segregare a utilizării cheilor pentru criptare date sau pentru sesiuni criptate.

Sistemul va audita acțiunile desfășurate în sistem, fie că sunt realizate de un utilizator, de un sistem extern sau de către sistem însuși (în cazul acțiunilor automate).

Se vor monitoriza cel puțin detalii privind momentul desfășurării acțiunii, utilizatorul, acțiunea desfășurată, entitate afectată și modificarea realizată.

Jurnalul de audit trebuie să permită sortarea, filtrarea și căutarea după diverse criterii, precum autorul acțiunii (utilizator sau sistem), acțiunile care au avut loc asupra unei anumite entități din sistem (ex. dosar, lucrare, document), acțiunile de un anumit tip etc.

Pentru documentele încărcate în sistem sau generate din sistem, se vor păstra toate versiunile acestora, împreună cu data și utilizatorul care a încărcat/generat documentul.

Sistemul va fi auditat și din perspectiva datelor cu caracter personal. Vor fi generate jurnale privind accesarea unui anumit set de date cu caracter personal, astfel încât să existe un control continuu asupra utilizatorilor care au accesat aceste date.

5. 2 Dezvoltare software securizată

Este bine cunoscut faptul că este mult mai puțin costisitor să construim un software securizat decât să corectam problemele de securitate după ce pachetul software a fost finalizat.

Astfel, toate cerințele menționate mai jos trebuie să fie integrate în ciclul de viață al dezvoltării ECRIS.

Atât dezvoltatorii interni, cât și resursele externe trebuie să fie informate cu privire la aceste practici de codificare securizate de bază. Arhitectura software cu toate detaliile specifice acestei arhitecturi trebuie să fie realizată ținând cont de cerințele de mai jos și de rezultatul analizei de risc efectuate de către dezvoltatorul soluției ECRIS.

Scopul securității codului este acela de a menține confidențialitatea, integritatea și disponibilitatea datelor din cadrul ECRIS. Acest obiectiv este atins prin punerea în aplicare a controalelor tehnice de securitate specifice.
Defectele de securitate software pot fi introduse în orice etapă a ciclului de viață al dezvoltării software:

- Slaba identificare a cerințelor de securitate în faza de proiectare
- Crearea unor modele conceptuale care au erori logice
- Utilizarea unor practici de codificare slabe care introduc vulnerabilități tehnice
- Implementarea software-ului în mod necorespunzător
- Introducerea defectelor în timpul întreținerii sau actualizării

Defectele de securitate ale software-ului pot afecta din punct de vedere al securității oricare dintre următoarele componente:

- Software-ul și informațiile asociate
- Sistemele de operare ale serverelor asociate
- Baza de date
- Alte aplicații într-un mediu partajat
- Sistemul utilizatorului
- Alte software-uri cu care utilizatorul interacționează

Principiile comune de securitate pentru dezvoltarea unui sistem ECRIS securizat sunt:

- Economia mecanismului – Păstrați codul și designul simplu. Elementele de configurare, de asemenea, ar trebui să fie cât mai simple posibil;
- Siguranță în mod implicit - acțiunea implicită pentru orice solicitare ar trebui să fie de a refuza acțiunea, în cazul în care o solicitare de utilizator nu reușește, sistemul rămâne sigur;
- Design deschis – designul nu trebui să fie un secret, opus față de "securitate prin obscuritate";
- Separarea privilegiilor – nu permiteți efectuarea operațiilor in aplicație bazat doar pe o condiție. De exemplu: nu este suficient ca utilizatorul să fie doar autentificat ci are nevoie si de o autorizare corespunzătoare.
- Cele mai mici drepturi comune – minimizați resursele partajate în interiorul aplicației.
- Acceptabilitate psihologică – Dacă software-ul securizat proiectat nu este ușor de utilizat, acesta nu va fi utilizat.
- Utilizarea software standard – utilizarea formatelor de date standardizate, bibliotecilor, cadrelor, aplicațiilor asigură o intercompatibilitate ușoară și actualizări regulate de securitate.

Pentru identificarea cerințelor specifice pentru aplicații web, validarea datelor de intrare, validarea datelor de ieșire, mecanisme de autentificare, administrarea sesiunii, managementul fișierelor, jurnalizare audit și tratarea erorilor precum și pentru managementul memoriei și securitatea bazelor de date se vor aplica recomandările OWASP Secure Coding Practices Quick Reference Guide (https://owasp.org/www-project-secure-coding-practices-quick-reference-guide/migrated_content).

Cerințele minime obligatorii sunt:

- Definirea și integrarea politicilor de securitate în ciclul de dezvoltare software al aplicației ECRIS. Securitatea informațiilor trebuie să fie parte integrantă din procesul de dezvoltare software al ECRIS. Trebuie luate în considerare toate aspectele relevante pentru securitate,

cum ar fi practicile de codificare securizată, securitatea mediului de dezvoltare, revizuirile codurilor etc. pentru realizarea unei aplicații ECRIS sigură.

- Toate persoanele implicate în echipa de dezvoltare trebuie să fie conștiente de responsabilitatea lor pentru dezvoltarea software-ului securizat. În acest scop, trebuie definite roluri adecvate și trebuie să se efectueze cursuri de formare adaptate publicului țintă.
- Criteriile de verificare a securității software în timpul dezvoltării trebuie definite pentru a determina dacă software-ul rezultat îndeplinește așteptările de securitate.
- Accesul la codul sursă trebuie atribuit pe baza principiului privilegiilor cel mai mic și verificat pentru a preveni modificările neautorizate sau neintenționate care pot duce la afectarea securității software.
- Verificarea integrității software prin semnarea codului sau integrarea altor mecanisme de asigurare a integrității de-a lungul procesului DEVOPS.
- Pe tot parcursul ciclului de dezvoltare trebuie să se determine la ce amenințări este expus software-ul în timpul producției și atenuarea acestor riscuri prin proiectarea software-ului. **Raportul de analiză și modelare a amenințărilor trebuie să facă parte din lista de livrabile standard ECRIS**
- Trebuie utilizate practici de programare sigure adecvate limbajului și mediului de dezvoltare. Vor fi respectate cel puțin recomandările OWASP Secure Coding Practices Quick Reference Guide (https://owasp.org/www-project-secure-coding-practices-quick-reference-guide/migrated_content).
- Revizuirea și/sau analizarea manuală a codului sursă (code review) și analiza automată în vederea identificării vulnerabilităților (Malicious code analysis) și pentru verificarea conformității cu cerințele de securitate specifice ECRIS. Raportul de testare statică (Static Application Security Testing - SAST) a aplicației trebuie să facă parte din lista de livrabile standard ECRIS. Detectarea rapidă a vulnerabilităților reduce expunerea pentru posibile atacuri. Nu este permisă punerea în producție a unei versiuni noi de aplicație fără să existe acest raport și acordul responsabilului tehnic al beneficiarului.
- Dezvoltarea aplicației trebuie efectuată într-un mediu izolat. Orice eroare apărută în mediul de dezvoltare nu trebuie să afecteze sub nicio formă mediul de producție.
- În conformitate cu reglementările RGPD (Regulamentul General privind Protecția Datelor) pe tot parcursul ciclului de dezvoltare software trebuie implementate măsuri tehnice și organizaționale care să asigure protecția datelor cu caracter personal (principiul '*data protection by design*'). Procesarea datelor cu caracter personal trebuie să se facă implicit cu cea mai mare protecție a vieții private a persoanei (principiul '*data protection by default*').

5.3 Semnăturа si sigiliul digital (electronic)

5.3.1 Semnătura digitală

Noul portal ECRIS trebuie să asigure funcționalități complete pentru semnarea individuală sau la grămadă a documentelor generate, stocate sau administrate prin intermediul portalului intern. Dacă utilizatorul autentificat în ECRIS are certificat digital valid atunci vor fi activate opțiunile de adăugare a semnăturii digitale. Portalul ECRIS va folosi informațiile disponibile în directorul LDAP integrat pentru identificarea utilizatorilor care au certificat digital valid.
Cerințele specifice implementării sistemului de semnături digitale sunt:

- Soluția de semnare digitală trebuie să fie strict legată de fluxul de documente în ECRIS și să permită adăugarea semnăturii la finalizarea fluxului sau în puncte intermediare de aprobare.

- Semnarea digitală trebuie să se realizeze într-un mod securizat, direct în token-ul criptografic și doar după introducerea PIN-ului de către posesorul token-ului .
- Soluția trebuie să permită crearea automată de versiuni noi a documentelor semnate.
- Documentele standard de tip Formular din ECRIS trebuie să includă automat delimitatorul de adăugare semnătură digitală (place holder). Pentru documentele non standard acesta trebuie definit de utilizator.
- Documentele semnate digital vor fi salvate în format PDF indiferent de formatul sursă al documentului. Conversia trebuie să se realizeze automat în ECRIS.

Procesul de semnare digitală trebuie implementat complet în ECRIS. Nu se acceptă adăugarea de componente software adiționale pe stațiile de lucru ale utilizatorilor. Singura excepție este legată de driverul de utilizare Smart Card sau USB Token.

5.3.2 Sigiliu electronic

Acesta este sinonim cu stampila institutiei si are un regim separat de Semnatura Digitala, reprezenantand practic institutia, nu o anumita persoana.
Cerintele de Securitate sunt impartite in trei categorii:

5.4 Securitatea stocarii si auditarii datelor/documentelor

5.4.1 Securizarea datelor stocate

Sistemul trebuie să ofere, într-un mod transparent pentru utilizator, protecția datelor digitale stocate de aplicație, atât cele stocate la nivelul bazelor de date, cât și al documentelor din sistemul de gestiune documente electronice, folosind mecanisme de protecție specifice fiecărei platforme în parte și includ:
- Criptare la nivelul discului fizic pe care sunt stocate datele
- Criptare la nivelul bazei de date
- Criptare la nivelul sistemului de fișiere

Un utilizator (administrator) care accesează baza de date sau sistemul de gestiune al documentelor direct, nu ar trebui să poată vedea datele în clar, decât prin mecanisme specifice aplicației (cu accesul controlat prin permisiuni și jurnalizat).

5.4.2 Securizarea configurărilor specifice aplicației

Cod: L2.2.1.A.SEC.CNF.9
Descriere generală
Sistemul trebuie să ofere posibilitatea de a securiza toate configurările specifice aplicației stocate la nivel de fișier (web.config, app.config, etc) prin mecanisme care să nu permită citirea lor în clar de către administratorii de sistem.
Configurările care vor fi criptate includ:
- Conturi de utilizator și parole
- Chei de acces la diversele resurse ale aplicației
- String-uri de conectare (ex: la baza de date)
- Configurări specifice aplicației care sunt stocate la nivel de fișier de configurare

Accesul la configurări ar trebui să fie controlat prin mecanismul de distribuire software și securizat doar la nivelul contului aplicativ specific (ex: prin certificate de tip machine key).

5.4.3 Securizarea configurărilor aplicației prin acces de pe stație controlată

Sistemul trebuie să ofere posibilitatea de a se efectua modificări asupra configurației (inclusiv distribuirea de actualizări) doar de pe statii dedicate (dupa MAC/IP).

5.4.4 Securizarea prin dezactivarea de protocoale și mecanisme de criptare depășite tehnologic

Sistemul trebuie să ofere posibilitatea administratorilor de a dezactiva în mod automat protocoale de securitate și mecanisme de criptare care sunt considerate de industria IT ca nesigure (ex: SSL3, TLS 1.0, TLS 1.1, MD5, 3DES), pentru a proteja sistemele de atacuri care vizează mecanismele mai vechi de securizare

5.4.5 Trasabilitate

Sistemul trebuie să asigure trasabilitatea completă a tuturor acțiunilor și modificărilor efectuate în cadrul sistemului, inclusiv la nivel de operații de citire. Sistemul trebuie de asemenea să asigure trasabilitatea operațiunilor complexe care pot afecta mai multe înregistrări (spre exemplu: operația de repartizare aleatorie a dosarelor în instanță). În corelare cu principiile de securitate, sistemul trebuie de asemenea să asigure și trasabilitatea operațiunilor eșuate din lipsa drepturilor de acces care pot indica tentative frauduloase de accesare a unor informații.

5.4.6 Securitatea librăriilor utilizate în cadrul aplicației

În cazul utilizării de librării dezvoltate extern pentru aplicațiile din cadrul sistemului ECRIS, se va ține cont de versiunile folosite, astfel încât să se evite:
- Utilizarea de librării învechite, care nu mai corespund realităților de Securitate
- Utilizarea de librării care au vulnerabilități cunoscute și a căror utilizare nu este recomandată

Toate librăriile utilizate, împreună cu codul dezvoltat vor fi scanate de vulnerabilități folosind mecanisme de analiză a codului sursă și identificare de vulnerabilități de securitate.

5.4.7 Monitorizare și jurnalizare

5.4.7.1 Gestionare centralizată a elementelor monitorizate

Sistemul trebuie să pună la dispoziție administratorilor mecanisme de vizualizare a elementelor monitorizate, a stării lor (healthy, degraded, etc) într-un format grafic, ușor de urmărit, astfel încât să poată fi identificate elementele care sunt cu probleme.
Sistemul va pune la dispoziția utilizatorilor mecanisme de codificare prin culori a stărilor diferitelor elemente monitorizate, astfel încât să fie ușor identificabile cele cu probleme.

5.4.7.2 Monitorizare aplicație

Sistemul trebuie să ofere instrumente de monitorizare pentru aplicațiile dezvoltate, atât la nivel de server de aplicație (web server) dar și la nivel de procese specifice aplicației.
Sistemul de monitorizare va permite monitorizarea parametrilor specifici aplicației, care includ:
- Monitorizarea punctelor expuse via HTTPS (Endpoint monitoring)
- Monitorizarea timpilor de încărcare pentru paginile web

- Monitorizarea certificatelor SSL/TLS pentru expirare
- Monitorizarea serverului de aplicație (disponibilitate, erori)

5.4.7.3 Monitorizare baze de date

Sistemul trebuie să ofere instrumente de monitorizare pentru parametrii de la nivelul bazei de date și includ:
- Capacitatea de stocare a bazei de date
- Volumele de tranzacții procesate concurent
- Performanța interogărilor pe baza de date
- Conflictele de tip deadlock apărute

5.4.7.4 Mecanisme de alertare a administratorilor

Sistemul trebuie să ofere posibilitatea administratorilor de a defini alerte în cazul în care se îndeplinesc anumite criterii (ex: încărcarea discului depășește 90% și poate deveni o problemă). Administratorii vor avea posibilitatea de a seta mai multe astfel de tipuri de notificări, în funcție de necesități.
Notificările vor fi transmise prin email sau vor fi disponibile în interfața de administrare a uneltei de monitorizare pentru consultare.

5.4.7.5 Jurnalizarea erorilor de aplicație

- Sistemul trebuie să ofere capabilități de jurnalizare a erorilor de aplicație, în funcție de severitatea acestora. Nivelul la care se face jurnalizarea va fi configurabil și se va putea face la unul din următoarele nivele de severitate: fatal, erori, alerte, debug, informativ, descriptiv.
- Erorile vor înregistra, pe lângă mesajul specific de eroare și modulul (componenta software) care a generat eroarea, pe ce sistem a fost generată, ce utilizator era logat, data și ora aferente.
- Sistemul va permite administratorilor consultarea informațiilor disponibile referitoarea la erorile generate de aplicație, cu posibilități de filtrare, căutare, etc.
- Detaliere erori de aplicație
- Sistemul trebuie să ofere capabilități de detaliere a erorilor de aplicație cu mesaje de eroare descriptive care sa conțină minim: stare endpoint serviciu, proces apelant, timp de răspuns, momentul înregistrării etc.
    - ✓ Înregistrările de jurnalizare trebuie să conțină minimum detalii despre:
        - ➢ ID-ul Sesiunii la care se referă mesajul
        - ➢ ID-ul modulului/aplicației care a generat mesajul
        - ➢ ID-ul utilizatorului logat in momentul generării mesajului
        - ➢ ID-ul mesajului generat
        - ➢ Severitatea mesajului
        - ➢ Data și ora la care a fost generat mesajul in format YYYY-MM-DD HH-MM-SS

Toate informațiile de mai sus trebuie să fie colectate în componenta de management al jurnalelor de audit pentru asigurarea unui mediu de stocare centralizat unic care să asigure integritatea datelor și stocarea pe termen lung.

5.4.7.6 Managementul sesiunii

Pentru a menține starea autentificată și a urmări progresul utilizatorilor în cadrul ECRIS, acesta va furniza utilizatorilor un identificator de sesiune (ID sesiune sau simbol) atribuit la momentul creării sesiunii și partajat de utilizator și de aplicația web pe toată durata sesiunii.
Odată ce o sesiune autentificată a fost stabilită, ID-ul sesiunii (sau token-ul) este temporar echivalent cu cea mai puternică metodă de autentificare utilizată de utilizator în ECRIS.
Soluția de management a sesiunii trebuie să permită deconectarea automată a utilizatorilor în cazul în care nu a mai efectuat nicio tranzacție într-o anumită perioadă de timp;
Sistemul să permită administratorilor terminarea manuală a sesiunilor utilizatorilor astfel încât un super-user să poată termina la cerere anumite sesiuni.
Soluția propusă pentru managementul accesului la sistemul ECRIS trebuie să accepte segregarea pe roluri a atribuțiilor de administrare pentru toate funcțiile / modulele din ECRIS.
Managementul rolurilor trebuie să permită acordarea de permisiuni în aplicație pe baza contextului creat la autentificare.
Atribuirea de drepturi și roluri in aplicație se poate face de către responsabilii de servicii ECRIS prin intermediul unor fluxuri de lucru cu aprobare ierarhică
Gestionarea de roluri trebuie să asigure următoarele funcționalități:

- Atribuirea utilizatorilor către mai multe roluri.
- Atribuirea utilizatorilor către roluri ierarhice.
- Trebuie să permită specificarea unor roluri care exclud alte roluri pentru a preveni atribuirea de roluri care s-ar afla în conflict.
- Permite atribuirea, pentru unii utilizatori, de drepturi de acces diferite de cele corespunzătoare rolurilor respectivilor utilizatori.
- Permite atribuirea de drepturi de acces individuale, distincte, pe lângă cele definite în cadrul rolului.
- Poate schimba dinamic și automat drepturile de acces în funcție de schimbările din rolurile utilizatorilor.
- Suporte noțiunea de „roluri persistente” (adică schimbările făcute definiției unui rol sunt aplicate tuturor utilizatorilor sub același rol).
- Suporte mutarea unui utilizator dintr-un rol în altul, impactul fiind modificarea drepturilor de acces corespunzătoare noului rol.
- În funcție de nevoie se vor crea roluri de tip doar-citire cu scop de consultare și auditare
- Oportunitatea atribuirii de noi roluri sau drepturi suplimentare pentru anumiți utilizatori este analizată de responsabilul de servicii ECRIS.
- Toate acțiunile de creare, modificare sau ștergere drepturi sau roluri trebuie auditat complet în sistemul de management al jurnalelor de audit
- La orice moment în timp trebuie să existe posibilitatea generării de rapoarte detaliate cu drepturile asociate fiecărui utilizator sau rol.
- Permite inițierea periodică a unui proces de revizuire a drepturilor de acces pentru utilizatorii selectați.

Sistemul ECRIS va implementa un mecanism securizat de control al accesului la toate interfețele API disponibile. Acest mecanism trebuie să asigurare controlul accesului pentru interfețe tehnice (nu avem utilizatori asociați acestor roluri) și trebuie să permită auditarea comenzilor efectuate prin intermediul acestor interfețe
Dat fiind gradul de confidențialitate al datelor din cadrul ECRIS acestea trebuie să fie stocate criptat în bazele de date, pe servere sau pe orice alt mediu digital.
Cerințe specifice:

- ✓ Criptarea datelor la stocare trebuie să includă orice locație în care ECRIS poate stoca date fie că e vorba de baze de date, discuri virtuale sau fizice ori medii de arhivare sau backup.
- ✓ Datele trebuie sa fie criptate folosind algoritmi de criptare standard recunoscuți în industrie.
- ✓ Criptarea datelor trebuie sa se facă întotdeauna folosind criptografie simetrica pentru volume mari de date precum criptarea întregii baze de date sau a mașinii virtuale.
- ✓ Utilizarea unui serviciu comun de management al cheilor bazat pe Key Management Interoperability Protocol (KMIP) este obligatoriu în vederea stocării pe un mediu extern securizat a cheilor simetrice.
- ✓ Cheile trebuie sa aibă proprietari bine definiți (legate de identități reale) și să respecte politicile de management al cheilor (vezi capitolul Politici de securitate și audit)
- ✓ Cheile vor fi actualizate periodic (rotite) pe parcursul perioadei de viață a acestora. Frecvența se va stabili de către beneficiari prin intermediul politicilor de securitate, dar nu trebuie să fie mai mare de 1 an.
- ✓ Cheile trebuie să fie transferate doar peste canal securizat (vezi Securitatea datelor in tranzit)
- ✓ Cheile trebuie să fie stocate pe un dispozitiv securizat de tip Hardware Security Module – HSM

Criptarea dublă trebuie aplicată pentru toate datele stocate in sistemul ECRIS. De exemplu, daca avem o bază de date ce folosește criptarea transparentă a datelor la nivel de fișiere trebuie să fie asigurată și criptarea discului pe care acestea baza de date este stocată.

5.5 Securitatea accesului la date si documente

5.5.1 Securizarea accesului în aplicație (autentificare)

Sistemul trebuie să pună la dispoziția utilizatorilor accesul la aplicație într-un mod securizat utilizând mai multe mecanisme de verificare a identității utilizatorilor, cum ar fi:
- Cont de utilizator și parolă (dintr-un sistem centralizat de management al identității, ex: Active Directory sau similar)
- Certificate utilizator
- Validare OTP prin SMS, e-mail

Accesul în aplicație nu trebuie permis utilizatorilor care nu sunt autentificați (conform unui mecanism de mai sus).

5.5.2 Sistem de identitate (Identity Provider)

Pentru autentificarea utilizatorilor și aplicațiilor în cadrul sistemului ECRIS Instanțe este necesară implementarea unui sistem de identitate (Identity Provider). Acest sistem va fi un sistem de tip Single Sign-On pentru toate aplicațiile dezvoltate în cadrul sistemului ECRIS. Sistemul va permite ca utilizatorii să poată folosi un singur cont de utilizator pentru a accesa orice aplicație din sistemul ECRIS, în funcție de drepturile pe care le au.
Acest sistem trebuie să implementeze cel puțin un standard deschis de autentificare (spre exemplu OAuth 2.0) astfel încât integrarea cu aplicațiile dezvoltate să fie ușor de realizat. Toate aplicațiile din sistemul ECRIS vor folosi serviciile sistemului de identitate pentru autentificarea utilizatorilor și nu vor implementa propriile mecanisme de autentificare. Autorizarea accesului la resurse va fi implementată la nivelul fiecărei aplicații și API.

Sistemul trebuie să ofere facilități clasice de înregistrare, resetare a parolei etc precum și posibilitatea autentificării de tip multi-factor (ex: parolă și SMS / email). Sistemul trebuie să permită posibilitatea de a asocia un certificat digital contului unui utilizator (respectiv asocierea cheii publice cu un cont). Această funcție este necesară pentru asigurarea funcționalității de validare a semnăturilor electronice. De asemenea pentru utilizatorii care dețin un certificat digital, acesta ar trebui să poată fi folosit inclusiv pentru autentificare.
Sistemul trebuie să ofere funcționalități de validare a identității. Această cerință este necesară pentru a valida identitatea terților care vor interacționa online prin intermediul portalului. Procesul de validare a identității este descris în cerințele funcționale.
Ofertantul trebuie să prezinte în cadrul propunerii tehnice tehnologiile/produsele utilizate pentru indeplinirea cerintelor, modul in care acestea vor fi adaptate specificului cerintelor, precum si eventalele constrangeri tehnologice care ar putea impiedica implementarea cerintelor in forma dorita de furnizor, propunand in acest caz solutii alternative.

5.5.3 Securizarea accesului la modulele aplicației (autorizare)

Sistemul trebuie să pună la dispoziția utilizatorilor accesul la diverse module ale aplicației pe baza drepturilor de acces descrise in profilul utilizatorului.
Administratorii vor avea posibilitatea de a defini roluri multiple de securitate, la nivel de ecran, la nivel de componentă logică (ex: dosar / lucrare) și la nivel de operație efectuată (citire, scriere, modificare, ștergere, printare).
Utilizatorii vor putea fi asociați la rolurile definite la nivelul fiecărei componente a sistemului și vor primi drepturi în aplicație în funcție de acestea.
Aplicația trebuie sa permită ca ulterior, utilizatorii sa primească drepturi suplimentare sau sa li se restrângă drepturile, in funcție de nevoile specifice.

5.5.4 Securizarea accesului aplicației la componentele sistemului de operare

Sistemul trebuie să pună la dispoziția administratorilor mecanisme prin care aplicația să poată fi folosită folosind un set minimal de permisiuni de acces la nivelul sistemului de operare și a infrastructurii de aplicație.
Utilizarea aplicației va trebui să fie posibilă și fără conturi cu drepturi administrative asupra sistemului de operare (ex: local administrator, domain administrator, etc).

5.5.5 Securizarea sesiunilor prin stabilirea unui timp de expirare (time-out)

Sistemul trebuie să pună la dispoziția utilizatorilor un mecanism de deconectare configurabil a sesiunilor inactive după expirarea unui interval de timp prestabilit. Utilizatorii vor trebui să își reconfirme identitatea prin mecanismele de autentificare specifice sistemului.
Perioada de inactivitate va putea fi definită de către administratorii instituțiilor utilizatoare, în limitele definite de la nivelul central al sistemului.
instituțiilor utilizatoare, în limitele definite de la nivelul central al sistemului.

5.5.6 Managementul sesiunii

Pentru a menține starea autentificată și a urmări progresul utilizatorilor în cadrul ECRIS, acesta va furniza utilizatorilor un identificator de sesiune (ID sesiune sau simbol) atribuit la momentul creării sesiunii și partajat de utilizator și de aplicația web pe toată durata sesiunii.

Odată ce o sesiune autentificată a fost stabilită, ID-ul sesiunii (sau token-ul) este temporar echivalent cu cea mai puternică metodă de autentificare utilizată de utilizator în ECRIS.
Soluția de management al sesiunii trebuie să permită deconectarea automată a utilizatorilor în cazul în care nu a mai efectuat nicio tranzacție într-o anumită perioadă de timp;
Sistemul să permită administratorilor terminarea manuală a sesiunilor utilizatorilor astfel încât un super-user să poată termina la cerere anumite sesiuni.
Soluția propusă pentru managementul accesului la sistemul ECRIS trebuie să accepte segregarea pe roluri a atribuțiilor de administrare pentru toate funcțiile / modulele din ECRIS.

5.5.7 Securizarea datelor prin mecanisme de validare a câmpurilor completate

Sistemul trebuie să ofere mecanisme de verificare a conținutului introdus de utilizatori care să detecteze și să elimine orice formă de cod executabil sau interpretabil, astfel încât să se asigure securitatea sistemului la atacuri prin injectarea de cod în câmpuri care mai apoi să fie executat la nivelul sistemului de operare, server de bază de date sau de aplicație.

5.5.8 Securizarea accesului la date pe rânduri

Sistemul va permite accesul la date pe baza rolului configurat în aplicație. Accesul la date va aplica un mecanism de filtrare a rândurilor de date returnate utilizatorului, pentru a asigura securitatea la nivel de obiecte specifice aplicației (ex: dosare / lucrări).
Utilizatorii care nu au acces la un anumit dosar / lucrare nu o vor vedea deloc în aplicație (nici în liste, nici în căutări).

5.5.9 Securizarea accesului la date prin API

Sistemul va permite accesul securizat la date prin API, astfel încât să se respecte mecanismele de autorizare specifice implementate în aplicație. Un utilizator nu va avea acces la date prin API mai mult decât este definit la nivelul rolului de securitate.

5.5.10 Gestiunea centralizată a certificatelor de criptare

Sistemul va permite gestionarea centralizată a certificatelor de securitate aferente sistemului, folosind mecanisme specifice:
- Autoritate de certificare (CA)
- Liste de certificate revocate
- Perioade configurabile pentru fiecare (tip de) certificat

Sistemul va permite rotirea periodică a certificatelor în mod centralizat, astfel încât administratorii să nu poată obține acces la cheile private de decriptare aferente certificatelor.
Actualizarea și distribuirea de certificate către mașinile destinație se va face în mod automat prin mecanisme programabile (ex: script).

5.5.11 Managementul identităților și autentificarea utilizatorilor

Autentificarea utilizatorilor în cadrul ECRIS joacă un rol foarte important în asigurarea securității sistemului în ansamblu. În cele ce urmează vor fi detaliate cerințele minime obligatorii pentru sistemul de management al identităților și autentificare în portalurile interne și externe ECRIS.

Sistemul trebuie sa ofere un Sistem de Management al Identitatilor integrat si care sa permita autentificarea personalului propriu. In acelasi timp pentru anumite categorii de utilizatori externi trebuie sa se permita autentificarea prin interogarea unor sisteme externe (ex. tabloul avocatilor).
Componenta de management al identităților pentru Portalul Intern ECRIS trebuie să îndeplinească următoarele cerințe minime și obligatorii:
• Managementul identităților trebuie realizat în conformitate cu politicile de securitate ale beneficiarului. Crearea, modificarea sau ștergerea utilizatorilor trebuie să respecte următoarele cerințe:

- Doar responsabilul de nivel business al ECRIS poate să solicite sau să aprobe aceste acțiuni;
- Toți utilizatorii și drepturile sau rolurile asociate acestora trebuie să fie documentate;
- În cazul în care acești utilizatori nu mai lucrează în organizație sau ocupă o altă funcție trebuie garantată ștergerea și respectiv actualizarea informațiilor și a permisiunilor asociate acestor utilizatori;
- Conturile de utilizator neutilizate pentru o perioadă lungă de timp trebuie reanalizate în vederea identificării necesității lor;
- Toate acțiunile efectuate pentru managementul identităților sunt jurnalizate în sistemul de management al jurnalelor de audit
    - ✓ Permite integrarea cu surse externe care stochează informațiile de identitate (precum un sistem HR, baze de date, fișiere, servere de directoare LDAP);
    - ✓ Fiecare cont de utilizator trebuie să aibă un identificator unic;
    - ✓ Permite delegarea responsabilității de administrare către alte direcții, departamente sau alte structuri organizaționale în funcție de necesitate;
    - ✓ Include un modul de fluxuri de lucru (workflows) care direcționează orice cerere către aprobatorul sau aprobatorii corespunzători;
    - ✓ Autentificarea utilizând mai mulți factori trebuie să fie implementată. Se recomandă combinația: utilizator, parola sau PIN, certificat digital.
    - ✓ Autentificarea trebuie efectuată în mai mulți pași (step-up authentication) astfel încât să permită flexibilitate în alegerea factorului de autentificare multiplă și pentru asigurarea unui nivel de acces limitat în cazul în care utilizatorul nu poate furniza toți factorii de autentificare necesari;
    - ✓ În funcție de mecanismele de autentificare configurate pentru fiecare utilizator acestuia îi este solicitat cel de-al doilea factor după introducerea contului de utilizator.
    - ✓ Managementul identităților va asigura implementarea politicii de securitate a parolelor în vederea garantării cerințelor de complexitate, istoric și valabilitate a acestora:
    - ✓ Utilizatorii vor avea acces la o interfață web securizată de administrare proprie (Self service) pentru:
- schimbarea parolei
- solicitarea unor actualizări de informații sau permisiuni în cadrul sistemului (aprobate ulterior pe baza de flux de lucru);
- schimbarea mecanismului suplimentar de autentificare (aprobat ulterior pe baza de flux de lucru);
    - ✓ Componenta de management al identităților include un modul de raportare ce permite căutarea și vizualizarea tuturor modificărilor efectuate pentru identitățile administrate
- Componenta de management al identităților pentru Portalul extern ECRIS trebuie să îndeplinească următoarele cerințe minime și obligatorii:
    - ✓ Fiecare cont de utilizator trebuie să aibă un identificator unic (ID) care să permită identificarea fără echivoc a acestuia.

- ✓ Implementarea unui mecanism de autentificare folosind mai mulți factori este opțional. Se poate implementa, de exemplu: utilizator, parola sau PIN, certificat digital, One Time Password (OTP) pe SMS sau email, etc.
- ✓ Autentificarea poate fi efectuată în mai mulți pași (step-up authentication) astfel încât să permită flexibilitate în alegerea factorului de autentificare multiplă și pentru asigurarea unui nivel de acces limitat în cazul în care utilizatorul nu poate furniza toți factorii de autentificare necesari;
- ✓ Implementarea unui flux securizat de înregistrare individuală a identităților prin intermediul unui schimb de mesaje de tip provocare-răspuns.
- ✓ Implementarea unei politicii de securitate a parolelor în vederea garantării cerințelor de complexitate, istoric și valabilitate a acestora politici de parole și de schimbare a acestora
- ✓ Utilizatorii vor avea acces la o interfață web securizată de administrare proprie (Self service) pentru:
  - schimbarea parolei
  - factorului de autentificare multiplă (număr de telefon, email, autentificator, etc.)
  - aflarea numărului de telefon
- ✓ Implementează un mecanism securizat de colectare și implementare a cererilor de ștergere a conturilor in conformitate cu prevederile GDPR. Dreptul persoanelor de a fi uitate, așa cum este el definit în Regulamentul General privind Protecția Datelor, trebuie să asigure transparență către utilizatori și să asigure trasabilitate asupra acțiunilor efectuate.

Soluția de autentificare propusă trebuie să ofere și proceduri de autentificare pentru serviciile web și aplicații ce depind de parteneri sau provideri externi, folosind mecanisme specifice cum ar fi SAML 1.0, 1.1, 2.0, ADFS, and WS-Federation sau OAuth;

5.5.12 Management al identităților pentru Portalul extern ECRIS

Componenta de management al identităților pentru Portalul extern ECRIS trebuie să îndeplinească următoarele cerințe minime și obligatorii:

- Fiecare cont de utilizator trebuie să aibă un identificator unic (ID) care să permită identificarea fără echivoc a acestuia.
- Implementarea unui mecanism de autentificare folosind mai mulți factori este opțional. Se poate implementa, de exemplu: utilizator, parola sau PIN, certificat digital, One Time Password (OTP) pe SMS sau email, etc.
- Autentificarea poate fi efectuată în mai mulți pași (step-up authentication) astfel încât să permită flexibilitate în alegerea factorului de autentificare multiplă și pentru asigurarea unui nivel de acces limitat în cazul în care utilizatorul nu poate furniza toți factorii de autentificare necesari;
- Implementarea unui flux securizat de înregistrare individuală a identităților prin intermediul unui schimb de mesaje de tip provocare-răspuns.
- Implementarea unei politicii de securitate a parolelor în vederea garantării cerințelor de complexitate, istoric și valabilitate a acestora politici de parole și de schimbare a acestora
- Utilizatorii vor avea acces la o interfață web securizată de administrare proprie (Self service) pentru:
  - ✓ schimbarea parolei
  - ✓ factorului de autentificare multiplă (număr de telefon, email, autentificator, etc.)

  - ✓ aflarea numărului de telefon
- Implementează un mecanism securizat de colectare și implementare a cererilor de ștergere a conturilor in conformitate cu prevederile GDPR. Dreptul persoanelor de a fi uitate, așa cum este el definit în Regulamentul General privind Protecția Datelor, trebuie să asigure transparență către utilizatori și să asigure trasabilitate asupra acțiunilor efectuate.

Soluția de autentificare propusă trebuie să ofere și proceduri de autentificare pentru serviciile web și aplicații ce depind de parteneri sau provideri externi, folosind mecanisme specifice cum ar fi SAML 1.0, 1.1, 2.0, ADFS, and WS-Federation sau OAuth;

5.5.13 Monitorizare utilizatori

Sistemul trebuie să ofere instrumente de monitorizare a activităților utilizatorilor, inspectând informațiile jurnalizate despre activitatea utilizatorului și alte informații disponibile și identificând șabloane referitoare la activitate suspectă (ex: încercarea de a accesa sistemul din afara rețelei, de pe mai multe stații în paralel).
Astfel de activități suspecte vor fi notificate administratorilor pentru a putea identifica eventualele vulnerabilități în interiorul organizației (ex: utilizatori care urmăresc preluarea sau modificarea neautorizată de date). Canalele de comunicare vor fi multiple (in aplicate si e-mail), nivelul si canalul de comunicare a alertelor vor fi configurabile.

5.5.14 Jurnalizare activități

Sistemul trebuie să asigure jurnalizarea tuturor activităților unui utilizator:

- Acces în sistem
- Schimbare parolă / detalii personale
- Consultare date
- Adăugare de date noi în sistem
- Toate operatiunile efectuate asupra datelor si documentelor existente în sistem

Sistemul va înregistra cel putin utilizatorul care a făcut modificarea, valoarea anterioară modificării, valoarea modificată, ce informații au fost consultate, de pe ce stație / IP, data și ora consultării / modificării.
Administratorii vor avea la dispoziție mecanisme de consultare raportare a acțiunilor jurnalizate prin care să poată identifica cu ușurință informațiile relevante.
Cerințele non-funcționale specifice aplicației ECRIS sunt detaliate în documentul L2.2.1.A-Cerinte non-functionale ale sistemului în capitolul dedicat AUD.Audit. Dintre aceste cerințe menționăm aici:

- Jurnalizarea activități. Sistemul trebuie să asigure jurnalizarea tuturor activităților unui utilizator în aplicația ECRIS cuprinzând cel puțin:
  - ✓ Accesul în sistem
  - ✓ Schimbarea parole și/sau detalii personale
  - ✓ Consultarea datelor
  - ✓ Adăugarea de date noi în sistem
  - ✓ Modificarea datelor existente în sistem
  - ✓ Ștergerea datelor existente în sistem
  - ✓ Sistemul va înregistra utilizatorul care a făcut modificarea, valoarea anterioară modificării, valoarea modificată, ce informații au fost consultate, de pe ce stație de lucru/IP, data și ora consultării / modificării.

- ✓ Administratorii vor avea la dispoziție mecanisme de consultare și raportare a acțiunilor jurnalizate prin care să poată identifica cu ușurință informațiile relevante (de ex: la un control tematic al Inspecției Judiciare).

5.6 Managementul jurnalelor de audit

Managementul jurnalelor de audit este o componentă cheie în cadrul întregului sistem de securitate al ECRIS prin faptul că asigură colectarea și corelarea informațiilor de audit generate de toate componentele. Această componentă va colecta informații de audit cel puțin din următoarele surse:
• Utilizarea portalul intern și public al aplicației ECRIS
• Utilizarea serviciilor API din cadrul ECRIS
• Soluțiile de monitorizare continuă (autentificarea utilizatorilor, accesul în sistem al conturilor privilegiate, managementul vulnerabilităților, etc)

Cerințele minimale pentru soluția de management al jurnalelor de audit sunt

- Să includă funcționalitățile de baza ale unei soluții de log management în vederea colectării centralizate și managementul logurilor;
- Colectarea logurilor trebuie să se facă fără a necesita instalarea unor agenți sau conectorilor pe sistemele sursă;
- Să aibă o singură interfață pentru toate funcționalitățile sale: căutare, raportare, configurarea regulilor de corelare și administrare;
- Să asigure salvarea tuturor datelor de intrare într-un singur sistem de stocare;
- Să aibă capacitatea de a menține amprenta de timp originală pentru fiecare eveniment;
- Să păstreze o copie a evenimentului original (raw event)
- Să permită căutarea după cuvinte cheie, intervale de timp, logica booleana (and, or, not …);
- Să permită efectuarea de căutări de tip „text liber” și expresii regulate ;
- Să permită executarea de funcții avansate statistice;
- Să permită definirea de rapoarte și tablouri de bord (dashboard) personalizate.
- Să permită automatizarea generării de rapoarte și trimiterea acestora pe email.
- Să aibă capacitatea de a corela datele de audit provenite din diferite surse;
- Să aibă capacitatea de a adăuga informații suplimentare datelor de audit prin intermediul corelării cu seturi de date locale;
- Să permită compresia automata a datelor, pentru a reduce spațiul de stocare;
- Trebuie să asigure control granular al perioadei de stocare în funcție de politica de retenție pentru tipuri diferite de date de intrare;
- Să permită retenția datelor pe termen lung, fără o limita specifică de timp, în funcție de spațiul de stocare disponibil alocat inițial și extins ulterior;
- Să permită arhivarea automată pe un mediu de stocare offline a datelor care au depășit perioada de retenție;
- Să permită restaurarea din arhivă a datelor vechi și includerea lor în procesul de căutare și raportare activă;

Volumetrie
ECRIS Instanțe
Soluția trebuie să asigure colectarea a minim **50 GB** de evenimente pe zi și să asigure disponibilitatea datelor pentru căutări active pentru cel puțin 1 an.
ECRIS Parchete

Soluția trebuie să asigure colectarea a minim **10 GB** de evenimente pe zi și să asigure disponibilitatea datelor pentru căutări active pentru cel puțin 1 an.

5. 7 Securitatea transferului datelor/documentelor

5.7.1 Securizarea datelor în tranzit

Sistemul trebuie să ofere, într-un mod transparent pentru utilizator, protecția datelor schimbate între diferitele părți ale sistemului (stații de lucru, servere de aplicație, servere de baze de date, diferite module ale aplicației, etc). Pentru criptarea datelor transferate prin rețele se va folosi minim protocolul TLS 1.2 sau similar (ex: IPSec).
Sistemul va permite utilizarea tehnologiilor de tip VPN (ex: comunicarea între diferitele instituții) ca mecanism suplimentar de securitate a datelor transmise.

5.7.2 Criptarea datelor in tranzit

Comunitatea criptografică internațională afirmă că punctele slabe ale versiunilor mai vechi ale protocolului TLS (TLS 1.0 / 1.1) reprezintă o amenințare iminentă pentru securitatea datelor în tranzit. Arhitectura ECRIS necesită ca toate punctele finale (End Points - EP) să utilizeze TLS 1.2 sau o versiune superioară cu suita de cifrare corespunzătoare. Pentru a aborda riscul, toate punctele de acces finale din ECRIS trebuie să dezactiveze versiunile TLS 1.1 sau mai vechi.
Obiectivele implementării securității în tranzit in cadrul ECRIS sunt:

- ***Obiective interne*** – Un punct de acces final intern *„Internal End Point (IEP)”* este definit ca orice punct final ale cărui conexiuni de intrare provin exclusiv din componentele sistemului ECRIS. De exemplu, se pot folosi punctele finale pentru comunicarea de la server la server, punctele finale care oferă clienți dedicate serviciilor etc.
- ***Obiective externe*** – Un punct de acces final extern *„External End Point (EEP)”* este definit ca orice punct final ale cărui conexiuni de intrare includ clienți în afara controlului aplicației. Un exemplu de obiective externe ar fi un punct de integrare cu alte sisteme din afara ECRIS.

Cerințe specifice minime obligatorii.
Toate punctele de acces din cadrul ECRIS, vor fi configurate după cum urmează:

- Versiunea TLS 1.2 sau mai nouă va fi activată împreună cu suita de cifrare corespunzătoare
- Certificarea ***SSLlabs A+*** trebuie obținută pentru toate punctele de acces externe.
- Versiunile TLS 1.0 sau TLS1.1 vor fi dezactivate.
- Pentru cazurile in care este necesara păstrarea unei versiuni mai vechi trebuie analizat si documentat impactul asupra securității întregului sistem. Această excepție trebuie avizată de către beneficiar pentru o perioadă limitată de timp, iar după expirarea acestui se solicită reevaluarea necesității păstrării excepției sau trecerea la versiunea TLS 1.2 sau mai noua.
- Toate punctele finale de acces expuse în Internet trebuie să folosească certificat SSL cu validare extinsă furnizat de către o autoritate de certificare recunoscută internațional.

Toate punctele finale de acces interne trebuie să folosească certificat SSL furnizat de către o autoritate de certificare recunoscută de către toți utilizatorii interni.
Securitatea datelor in procesare
Mecanismele de securitate a datelor în procesare implementate pentru sistemul ECRIS trebuie să se urmărească realizarea următoarelor funcții: identificare, autentificare, autorizare și auditarea.

5.8 Testarea securitatii

5.8.1 Testarea volumetrică a performantelor.

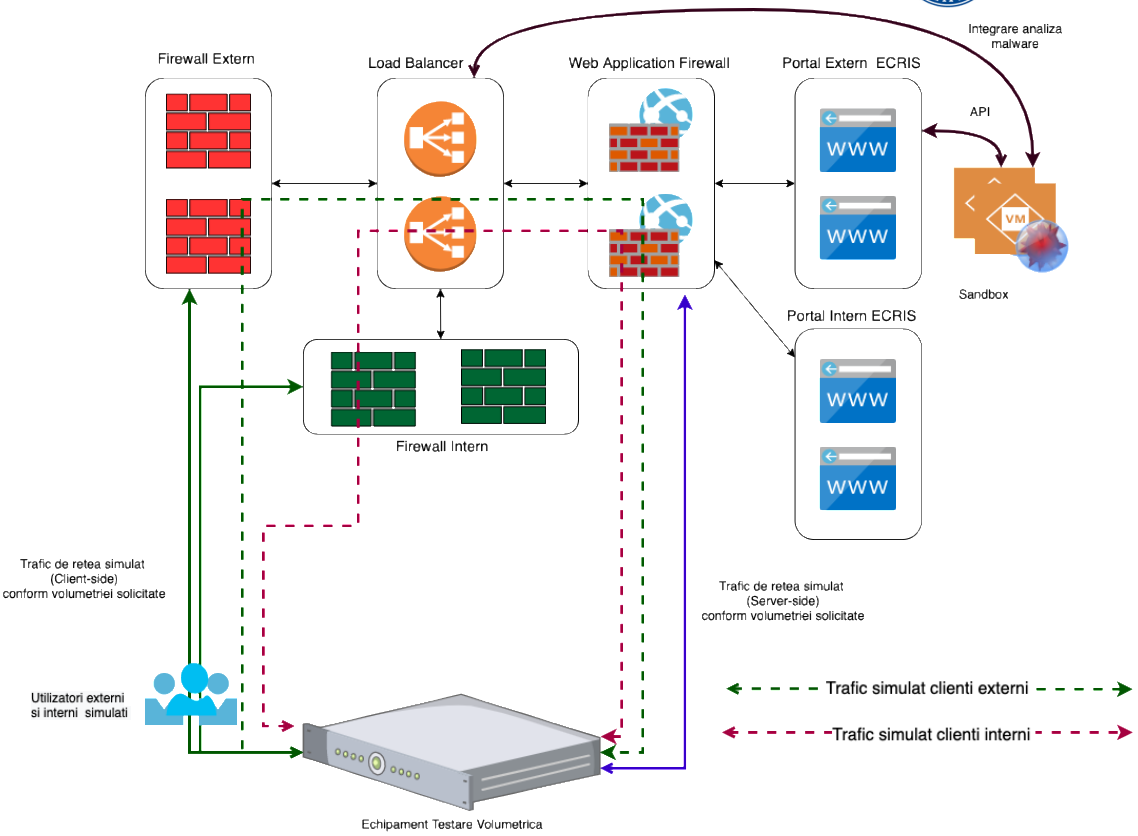
Evaluarea infrastructurii ECRIS

Înainte de punerea în producție a sistemului ECRIS se va realiza cel putin o sesiune de testare volumetrică a infrastructurii de rețea, inclusiv a soluțiilor de securitate perimetrală și a datelor în tranzit. Toate funcționalitățile de securitate solicitate în caiet vor fi activate și optimizate pe parcursul acestor teste. Scopul acestei testări este de a valida infrastructura de rețea și securitate pentru capacitățile și performanțele solicitate în caiet.

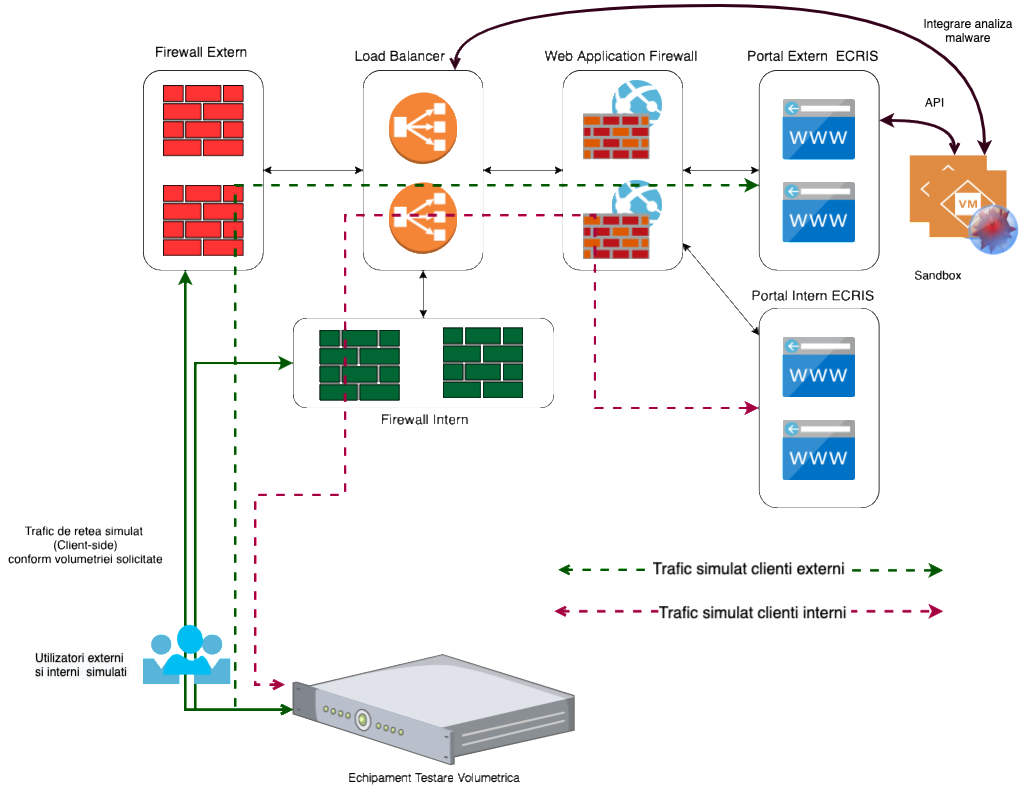
Aceste teste se vor realiza în configurație *2-arm* astfel încât să fie simulați atât clienții cât și serverele cu care aceștia interacționează, dar și în configurație *1-arm* în care se vor simula doar clienții iar conexiunile de rețea se vor termina în Portalul Intern și respectiv Portalul Extern ECRIS.

Soluția utilizată pentru efectuarea testelor trebuie să aibă următoarele caracteristici pentru a asigura o testare eficientă:

- trebuie să permită generarea de trafic ce conţine un amestec de protocoale la viteze de până la 10 Gb/s per port, folosind o pondere realistă a tipurilor de protocoale în cadrul traficului;
- trebuie să permită efectuarea testelor de stres asupra echipamentelor de securitate prin folosirea a peste 35.000 de tipuri de atacuri ce conţin malware şi prin simularea prezenţei botneţilor sau folosirea tehnicilor de eludare a securităţii;
- trebuie să permită particularizarea şi manipularea oricărui tip de protocol din cele suportate, inclusiv a datelor de tip „raw”;
- trebuie să permită generarea de pe un singur port simultan a următoarelor categorii de trafic: trafic legitim, trafic de tip DDoS şi trafic cu conţinut malware;
- trebuie să permită simularea de aplicaţii reale, fiecare configurabilă cu acţiuni pentru a permite simularea unui comportament multiuser şi a unui conţinut dinamic. Se vor simula aplicațiile explicit folosite în cadrul sistemului ECRIS cum ar fi: Web, SQL, streaming video;
- trebuie să permită găsirea problemelor de securitate dintr-o reţea şi efectuarea de teste de securitate într-un mod surprinzător prin folosirea unor tehnici rapide de tip „fuzzing” aplicate asupra diferitelor protocoale;
- trebuie să permită rularea a cel puţin următoarelor componente, adică tipuri de teste având următoarele caracteristici:
  - ✓ Simulator de aplicaţii – permite utilizatorilor să creeze un mix de aplicaţii şi să ruleze teste în “2-Arm mode” (sistemul fiind şi serverul şi clientul) pentru a testa echipamentele care pot analiza un astfel de trafic la nivel de aplicaţie;
  - ✓ Simulator de clienţi – permite userilor să genereze trafic de tip client către servere reale ce se doresc a fi testate (“1-Arm mode”), sistemul ofertat fiind clientul;
  - ✓ Teste de securitate – măsoară abilitatea unui echipament de a proteja un sistem prin transmiterea de trafic malitios către acesta şi a verifica dacă echipamentul respectiv blochează atacurile;
  - ✓ Teste de verificare a echipamentelor de protecţie a reţelei – permite generarea de trafic maliţios la scară largă, până la 10 Gbps per port, funcţie de licenţiere;
- Arhitectura de testare propusa este cea prezentată în diagrama de mai jos.



Figură 2. Arhitectura de testare volumetrică de performanță în configurație **2-Arm**



Figură 3. Arhitectura de testare volumetrică de performanță în configurație 1-Arm

Raportul detaliat al rezultatul testului volumetric de infrastructură este parte din livrabilele de proiect și trebuie să demonstreze că infrastructura susține throughput-ul și numărul de conexiuni solicitate în condiții de trafic real.

5.8.2 Testarea periodică a securității

Considerând gradul ridicat de securitate solicitat pentru datele procesate in ECRIS este absolut necesară revizuirea tehnică detaliată a sistemului pentru vulnerabilități și identificarea măsurilor necesare pentru acoperirea acestor vulnerabilități. Aceste teste sunt solicitate de asemenea în cadrul RGPD (Regulamentul General privind Protecția Datelor) în vederea asigurări protecției datelor cu caracter personal.
Cerințe de evaluare periodică a securității sistemului prin intermediul testelor de penetrare:

- Scopul realizării testelor de securitate de tip penetration testing este acela de a evalua buna implementare a măsurilor de securitate și a sistemului în ansamblul său.
- Testele de penetrare a securității trebuie să se desfășoare periodic, dar cel puțin odată pe an pe toată perioada de funcționare a sistemului ECRIS.
- Înainte de punerea în producție a sistemului ECRIS se va executa un test de penetrare de tip ”white box” atât pentru aplicația ECRIS cât și pentru toată infrastructura parte a acestuia.
- Testarea penetrării securității trebuie plasată în ansamblu în contextul sistemului de management al securității implementat pentru ECRIS.
- În vederea evaluării furnizorului de servicii de testare de penetrare acesta trebuie să prezinte metodologia folosită pentru tipul și scopul asociat și un exemplu de raport de testare.
- În cazul punerii in producție a unei actualizări majore de versiune pentru sistemul ECRIS trebuie reluate testele de evaluare a securității pentru modulele afectate din aplicație.
- Testele de penetrare se realizează manual plecând de la scanările periodice de evaluare a vulnerabilităților pentru sistemul ECRIS.
- Trebuie să includă și evaluarea de tip „social engineering” pentru a identifica riscurilor asociate nerespectării de către utilizatorii finali ai sistemului ECRIS a politicilor și procedurilor de securitate.
- Raportul de prezentare a rezultatelor testelor trebuie să includă o descriere detaliată a fiecărei vulnerabilități identificate și evaluate precum și a tuturor celorlalte probleme identificate.
- Raportul trebuie să prezinte riscurile mult mai specifice pe care le poate prezenta vulnerabilitatea, inclusiv metode specifice despre și în ce măsură poate fi exploatată
- Raportul trebuie să includă un indicator general de tip Risc Score pentru întreg sistemul evaluat

5.9 Managementul vulnerabilităților aplicațiilor Web

Evaluarea detaliată a vulnerabilităților asociate cu aplicațiile web de tip Portal ale sistemului ECRIS ne furnizează informații valoroase pentru asigurarea unei bune securități a acestor sisteme. Soluția propusă trebuie să acopere cel puțin top 10 OWASP.

Cerințe minime obligatorii:

- Soluția propusă trebuie să includă toate componentele necesare pentru testarea automată a vulnerabilităților aplicațiilor Web din cadrul ECRIS
- Asigură setarea credențialelor de autentificare în vederea testării secțiunilor protejate de autentificare. Mecanismele de autentificare suportate trebuie să permită autentificarea in portalurile interne și externe ECRIS.

- Permite realizarea unor scanări manuale sau automate de tip crawl pentru descoperirea structurii aplicației și afișarea rezultatelor scanării sub formă ierarhică (sitemap).
- Asigură identificarea și restricționarea funcției de logout din cadrul aplicației web supusă scanării.
- Asigură excluderea unor pagini și a unor parametri în cadrul procesului de scanare.
- Asigură elaborarea de rapoarte complexe pe baza unor șabloane predefinite și exportarea acestora în format PDF și CSV
- Oferă informații suplimentare despre vulnerabilitățile identificate, ce vor include și metode de remediere.
- Permite definirea de profiluri de scanare personalizate in vederea adaptării testelor efectuate pentru aplicația scanată.
- Permite vizualizarea și editarea atât a conținutului cât și a header-ului din cadrul cererilor și răspunsurilor HTTP
- Asigură clasificarea vulnerabilităților identificate după severitatea acestora și după impactul ce îl pot aduce în cadrul ECRIS.
- Trebuie să permită integrarea cu soluția de management al jurnalelor de audit

5.10 Anonimizarea sau mascarea datelor cu caracter personal

Cerințele minime pentru anonimizarea datelor cu caracter personal sunt:

- Documentele anonimizate de către instrumentul software vor fi verificate manual și de către utilizatori întinate de publicarea acestora.
- Utilizatorii vor avea posibilitatea de a compara versiunea inițială cu cea anonimizată prin intermediul unui instrument tehnic care va marca diferențele și zone de text care sunt susceptibile să conțină date cu caracter personal.
- Instrument tehnic de anonimizare să aibă o acuratețe bună pentru documentele statice în funcție de conținutul acestora.
- Anonimizarea se va baza pe datele structurate în primul rând de la nivelul dosarului despre părți. De multe ori în redactarea unei hotărâri datele se introduc manual, întrucât este mai rapid, așa că pot exista diferențe între datele structurate și textul hotărârii.
- Asigură identificarea automată a datelor cu caracter personal atât în date structurate (la nivelul dosarului din ECRIS) cât și în date nestructurate (textul hotărârii redactate manual)
- Suportă cel puțin următorii algoritmi de căutare a datelor cu caracter personal: expresii regulate (RegEx), valori din dicționar și filtre pe coloane pentru datele structurate;
- Suportă cel puțin următorii algoritmi de anonimizare a datelor ce vor fi utilizați selectiv în funcție de cerințele legale:
  - ✓ criptare cu păstrarea formatării
  - ✓ redactare prin mascarea unui șir de caractere conform unor specificații date
  - ✓ filtrare parțială prin omiterea unor caractere
  - ✓ generarea unor valori aleatorii.
- Permite crearea de reguli personalizate de identificare și anonimizare a datelor cu caracter personal
- Asigură integrarea cu baza de date a sistemului ECRIS pentru identificarea automată și anonimizarea datelor;

- Anonimizarea trebuie sa fie consistentă în contextul unui document (de exemplu: Partea1 să fie întotdeauna anonimizată Anon1 iar Partea2 să fie întotdeauna anonimizată Anon2) pentru a asigura același nivel de înțelegere pe document.
- Asigură identificarea automată și anonimizarea datelor in fișiere nestructurate de tip: text, PDF (text) și Microsoft Office
- Asigură integrarea cu soluția de management a logurilor pentru monitorizarea tuturor activităților efectuate.

Cerințe tehnice minimale pentru instrumentul tehnic de anonimizare dinamică:

- Asigură mascarea dinamică a datelor la nivelul aplicației fără a modifica datele în baza de date
- Permite identificarea datelor cu caracter personal și aplicarea de politici de anonimizare direct la nivelul aplicației ECRIS fără sa necesite scrierea de cod sau module în aplicație.
- Permite crearea de politici de anonimizare personalizate în funcție de contextul utilizatorului autentificat în aplicație.
- Rulează automat procesul de anonimizare, odată ce au fost stabilite politicile, fără să aibă nevoie de intervenție umană
- Suportă cel puțin următorii algoritmi de anonimizare a datelor ce vor fi utilizați selectiv în funcție de cerințele legale:
  - ✓ criptare cu păstrarea formatării
  - ✓ redactare prin mascarea unui șir de caractere conform unor specificații date
  - ✓ filtrare parțială prin omiterea unor caractere
  - ✓ generarea unor valori aleatorii.
- Asigură integrarea cu soluția de management a logurilor pentru monitorizarea tuturor accesărilor de date. Datele de audit trebuie să includă detalii despre modul în care au fost prezentate datele către utilizatori.

6. Cerinte non-functionale

Cerintele non-funcţionale sunt impartite in urmatoarele categorii:

6.1 Scalabilitate si Performanta

6.1.1 Scalabilitate

Sistemul trebuie să fie scalabil și să permită extinderea capacităților de stocare si procesare conform nevoilor ulterioare (scale-up, scale-out). Sistemul de stocare prevăzut trebuie să asigure extinderea capacității de stocare.

6.1.2 Informații volumetrice

Sistemul propus trebuie să permită gestiunea cu succes a informațiilor aferente instituțiilor (număr de dosare, număr personal angajat), fără degradarea performanței.
Informațiile volumetrice referitoare la:

- Număr de dosare pentru fiecare instituție
- Personal dedicat în fiecare instituție (pe funcții: judecători, procurori, grefieri, etc)

6.1.3 Performanță

Noul sistem trebuie să fie unul performant. Operațiile uzuale trebuie să poată fi executate imediat și să respecte criteriile de performanță stabilite. Operațiile cu o frecvență mai rară trebuie să poate fi realizate într-un timp rezonabil.
Livrabilul L2.2.1.A-Cerinte non-functionale ale sistemului.pdf – capitolul 2.1.12

6.2 Business continuity (Disponibilitate, Balansare/Redundanta, Back-up, Restore, Disaster Recovery)

Asigurarea continuității activității
Sistemul ECRIS trebuie aibă o arhitectură cu caracteristici de redundanță care să permită continuarea operării în caz de avarii non-critice fără să se realizeze comutarea în locația BCDR.
În cadrul sistemului ECRIS trebuie inclus un sistem de backup și restaurare care trebuie să permită reconstituirea datelor și a stării sistemului la o dată anterioară.

6.2.1 Disponibilitate platformă

Sistemul trebuie fie proiectat astfel încât să asigure continuitate în exploatare și în cazul unor evenimente neprevăzute, de natură a afecta buna funcționare a sistemului. Sistemul trebuie aibă o arhitectură cu caracteristici de redundanță care să permită continuarea operării în caz de avarii non-critice (defecțiuni hardware, software, de comunicații).

6.2.2 Balansarea încărcării

Sistemul trebuie să permită funcționarea optimă prin implementarea de soluții de balansare/redistribuire a proceselor aplicației, fără a întrerupe funcționarea normală a aplicației.

6.2.3 Asigurarea disponibilităţii

Sistemul trebuie să fie proiectat hardware și software, astfel încât să nu existe puncte unice vulnerabile de tipul single point of failure (SPOF).
De asemenea, trebuie să asigure respectarea de către beneficiari a legislației privind protecția datelor prin:
• „Planuri de gestionare a riscurilor” pentru identificarea riscurilor, evaluarea potențialului impact al acestora și planificarea intervențiilor cu măsuri tehnice și organizatorice adecvate. Pe baza ultimelor evoluții tehnologice, aceste măsuri trebuie să asigure un nivel de securitate proporțional cu gradul de risc;
• „Planuri de continuitate a activității” și „planuri de rezervă și de redresare” pentru a institui procedurile necesare de asigurare a disponibilității funcțiilor în urma unui eveniment dezastruos și readucerea tuturor funcțiilor la situația normală cât mai curând posibil;

6.2.4 Backup

6.2.4.1 Realizarea de copii de siguranță

Sistemul trebuie să gestioneze situațiile în care este necesară restaurarea datelor, în cazul unor coruperi sau defecțiuni la sistemul de stocare a datelor. Sistemul va avea la dispoziție un sistem de arhivare de tip WORM (Write Once Read Many) prin care va putea prelua informațiile care urmează a fi arhivate, cu software-ul specific penru realizarea de copii de siguranță.

6.2.4.2 Realizarea de copii de tip Back-up

Sistemul trebuie să permită realizarea de copii a datelor de tip "back-up" folosind mai multe mecanisme specifice: backup full, diferențial cât și de log.

Backup

Atât documentele în sine cât și bazele de date ce conțin alte informații decât documente (spre exemplu metadate relative la documente), vor fi copiate pe un sistem de stocare pentru backup în vederea restaurării. Tehnologia de salvare/copiere a datelor va permite scrierea acestora în mod automat, după o politică ce va fi stabilită de către administratorii nodurilor ECRIS.
Capacitatea acestor dispozitive este proiectată în așa fel încât acestea să permită copii succesive ale datelor din dispozitivele SAN.

Politici de backup și arhivare pe termen lung

- Furnizorul soluției de arhivare și backup va defini împreună cu beneficiarii (ECRIS Instanțe și ECRIS Parchete) politicile de backup și arhivare a datelor.
- Furnizorul va implementa procesului de backup și arhivare astfel încât să se asigure automatizarea acestuia.
- Toate datele stocate în sistemul de backup și arhivare vor fi criptate.
- Cheia de criptare va fi administrată prin intermediul sistemului de management al cheilor de criptare.

În cazul în care benzile magnetice folosite pentru backup și arhivare pe termen lung sunt scoase din unitatea de lucru, acestea vor fi păstrate în condiții adecvate pentru asigurarea protecției la factori perturbatori de mediu. Se recomandă stocarea lor într-un mediu securizat fizic, protejat la acțiunea câmpurilor electromagnetice și cu temperatura constantă controlată.

6.3 Localizare

6.3.1 Utilizarea caracterelor românești

Sistemul trebuie să asigure implementarea suportului Unicode la nivelul întregii aplicații (web, baze de date, etc) pentru a putea accepta introducerea tuturor caracterelor specifice limbii române (diacritice).
Caracterele românești vor respecta standard-ul ISO 639-1:RO de codificare a limbii române cu caractere latinice.

6.3.2 Interfața grafică trebuie să fie în limba română

Sistemul trebuie să permită afișarea interfeței cu utilizatorul în limba română, pentru o înțelegere facilă a utilizatorilor.

6.3.3 Căutarea folosind caractere fără diacritice

Sistemul trebuie să permită căutarea în toate câmpurile aferente, fără să fie condiționată de scrierea cu diacritice (ex: la căutarea cu ”s” să fie returnate și rezultatele cu ”ș”).

6.4 Accesibilitate

6.4.1 Experiență de utilizator ergonomică și accesibilă

Sistemul trebui să propună o interfață utilizator cât mai ergonomică, bazată pe reducerea click-urilor, folosind un sistem de afișare unitar.
Interfața utilizator va respecta principiile din documentul de arhitectură UI/UX și va fi cât mai ușor de înțeles/utilizat. Elementele grafice afișate pe ecran vor fi intuitive, oferind informațiile necesare înțelegerii rolului lor de către utilizatori.
Sistemul trebuie să respecte standarde de accesibilitate aplicabile, cum ar fi:
- Directiva Europeană 2016/2012 referitoare la accesibilitatea site-urilor web ale instituțiilor publice
- Web Content Accessibility Guidelines (WCAG) 2.0

6.4.2 Accesibilitate pentru persoane cu dizabilități

Sistemul trebuie să fie accesibil persoanelor cu dizabilități vizuale și persoanelor ce suferă de surdocecitate, în vederea asigurării accesului neîngrădit al persoanelor cu dizabilități la funcțiile oferite de această aplicație. Trebuie să se poată mări dimensiunea fontului, contrastul ecranului, navigarea prin aplicație fără ajutorul mousului (folosind tastatura).

6.4.3 Independența de locația fizică

Portalurile publice ale sistemului trebuie să permită accesul indiferent de punctul fizic de acces, pe baza drepturilor/rolurilor stabilite la logarea în sistem.

6.4.4 Optimizarea în funcție de dispozitiv

Portalurile publice ale sistemului trebuie să optimizeze automat interfața (formatul elementelor, organizarea informației etc) în funcție de dispozitivul de pe care este accesată aplicația și rezoluția acestuia: PC, laptop, tabletă.

6.4.5 Interfață utilizator optimizată pentru rezoluție minimă

Sistemul trebui să ofere o interfață utilizator optimizată pentru o rezoluție minimă de 1366×768 pixeli, pentru a permite utilizarea și pe dispozitivele existente în cadrul instituțiilor.

6.5 Compatibilitate

6.5.1 Compatibilitatea navigatoarelor web

Sistemul trebuie dezvoltat folosind o tehnologie compatibilă cu versiunile curente de navigatoare web pentru care producătorii oferă suport (versiunile desktop și mobile), cel puțin pentru:

- Google Chrome
- Mozilla Firefox
- Microsoft Edge
- Apple Safari

6.5.2 Compatibilitatea cu versiuni ulterioare

Sistemul trebuie dezvoltat folosind o tehnologie care să permită in viitor migrarea pe platforme noi fără a limita alegerea producătorului.

6.5.3 Compatibilitate utilitar de distribuire aplicații cu tipurile de sisteme de operare, baze de date și aplicații folosite

Sistemul trebuie să propună un sistem de distribuție a aplicațiilor și versiunilor de actualizare (DevOps) care să fie compatibil cu infrastructura software propusă (sisteme de operare, baze de date, platformă de dezvoltare) și să permită distribuirea de software pe platforma propusă.

6.5.4 Compatibilitate API-uri cu tehnologii standard

Sistemul trebuie să expună interfețe programabile (API) care să adere la tehnologii standard, cum ar fi OData, ORDS, gRPC, REST, etc, pentru a permite o integrare facilă a componentelor sistemului.

6.5.5 Catalog online API-uri cu tehnologii standard

Sistemul trebuie să expună un catalog online pentru toate interfețele programabile (API) expuse, cu descrierea funcționalităților și a metodelor expuse. Catalogul va include documentație în format standard (ex: Swagger) pentru fiecare metodă disponibilă din interfețele programabile.

6.6 Protecția datelor personale în contextul RGPD (Regulamentul General privind Protecția Datelor)

RGPD (Regulamentul General privind Protecția Datelor) sau GDPR (General Data Protection Regulation), cum mai este cunoscut, stabilește cerințele detaliate în ceea ce privește colectarea, stocarea și gestionarea datelor cu caracter personal. Acest regulament se aplică atât în cazul organizațiilor europene care prelucrează datele cu caracter personal ale cetățenilor din UE cât și în cazul organizațiilor din afara UE care vizează cetățeni din UE.
Legislația aplicabilă în România pentru protecția datelor personale în cadrul sistemului judiciar sunt:
• Legea nr. 190/2018 privind măsuri de punere în aplicare a Regulamentului (UE) 2016/679 al Parlamentului European și al Consiliului din 27 aprilie 2016 privind protecția persoanelor fizice în ceea ce privește prelucrarea datelor cu caracter personal și privind libera circulație a acestor date și de abrogare a Directivei 95/46/CE (Regulamentul general privind protecția datelor)
• LEGE nr. 363 din 28 decembrie 2018 privind protecția persoanelor fizice referitoare la prelucrarea datelor cu caracter personal de către autoritățile competente în scopul prevenirii, descoperirii, cercetării, urmăririi penale și combaterii infracțiunilor sau al executării pedepselor, măsurilor educative și de siguranță, precum și privind libera circulație a acestor date.

În cadrul procesului de analiză a fost identificată în mai multe locuri nevoia de implementare a unor procese sau soluții tehnice de protecție a datelor cu caracter personal procesate în cadrul ECRIS, în special pentru componentele ce publică aceste informații spre Internet prin intermediul portalurilor publice.
Datele cu caracter personal identificate în cadrul procesului de analiză sunt enumerate mai jos.

- Nume complet
- Nume judecători

- Nume părți, participanți, martori
- Numele mamei si tatălui,
- CNP
- Adresa de domiciliu
- Adrese de email,
- numere de telefon, fax
- Conturi bancare
- Numere de înmatriculare ale autovehiculelor, navelor etc.
- Porecle/parole părți și martori
- Date de identificare militare
- Numere de brevete, licențe, livret militar,
- Număr licență de exercitare a unei profesii liberale etc.

Aceasta nu reprezintă o listă exhaustivă a tuturor datelor cu caracter personal din cadrul ECRIS.
Se va acorda o atenție specială prelucrărilor de date cu caracter personal care vizează categorii de date precum:
• date care dezvăluie originea rasială sau etnică, opiniile politice, filozofice sau religioase, apartenența sindicală;
• date privind sănătatea sau orientarea sexuală, date genetice sau biometrie;
• date referitoare la infracțiuni sau condamnări penale;
• date referitoare la minori.
În conformitate cu specificațiile RGPD operatorul datelor personale implementează măsuri tehnice și organizatorice adecvate, incluzând printre altele:
• capacitatea de a asigura confidențialitatea, integritatea, disponibilitatea și rezistența continuă a sistemelor și serviciilor de prelucrare;
• capacitatea de a restabili disponibilitatea datelor cu caracter personal și accesul la acestea în timp util în cazul în care are loc un incident de natură fizică sau tehnică;
• stabilirea unui proces pentru testarea, evaluarea și aprecierea periodică a eficacității măsurilor tehnice și organizatorice pentru a garanta securitatea prelucrării.
• Anonimizarea, pseudonimizarea și criptarea datelor cu caracter personal, după caz.
În cadrul sistemului ECRIS toate datele, inclusiv cele cu caracter personal, trebuie să fie stocate criptat pentru asigurarea confidențialității și integrității acestora.

Cerințele minime obligatorii ce trebuie respectate de componenta de protecție avansată antimalware:
• Soluția trebuie să permită utilizarea în mod integrat cu portalul ECRIS prin intermediul API, și cu componenta de protecție perimetrală NGFW sau de balansare a încărcării.
• Va oferi protecție pentru atacurile de tip „zero-day” chiar dacă protecția prin semnături din baze de date nu este disponibilă;
• Va analiza și detecta malware în documente Adobe PDF, fișiere MS Office, fișiere executabile și de tip arhivă;
• Va emula atacuri pentru multiple sisteme de operare, cel puțin pentru: MS Windows 8.1 și 10. Atât sistemele de operare cât și pachetul Microsoft Office incluse în mașinile virtuale care emulează fișierele vor fi copii licențiate Microsoft și vor fi incluse în soluție;
• Va emula fișiere cu mărime de până la 100 MB sau chiar mai mult;
• Permite partajarea automată a informației despre noile atacuri cu alte componente de securitate sub formă de semnături;
• Va permite inspectarea și blocarea atacurile via HTTPS prin intermediul integrărilor menționate;
• Va permite integrarea cu protocolul SMTP pentru a scana documentele atașate în email;
• Soluția va include un management centralizat pentru configurarea centralizată și distribuirea update-urilor către toate echipamentele de analiză
• Soluția trebuie să permită utilizarea regulilor de tip YARA.

• Soluția va fi implementată în arhitectură cu înaltă disponibilitate astfel încât în cazul în care unul dintre echipamentele hardware este defect soluția să funcționeze. Se acceptă degradarea performanțelor în perioada de indisponibilitate a unuia dintre echipamente.
• Soluția va include surse de alimentare și discuri redundante pentru asigurarea disponibilității înalte la nivelul echipamentelor
• Managementul echipamentelor se va face centralizat prin intermediul unei console unice de configurare, operare și raportare.

Volumetrie
ECRIS Instanțe
• Soluția trebuie să asigure administrarea centralizată a conturilor privilegiate din cadrul ECRIS Instanțe, inclusiv pentru infrastructura de suport și componenta BCDR.
• Soluția implementată pentru securizarea ECRIS Instanțe trebuie să permită scanarea a cel puțin 10000 fișiere unice pe ora în perioada de vârf și un total de 70000 de fișiere unice pe zi.
• Setul implementat la ECRIS Instanțe va include cel puțin două echipamente de protecție avansată și componenta de management centralizat în centrul principal de date și un echipament și componenta de management pentru locația BCDR

ECRIS Parchete
• Soluția trebuie să permită scanarea a cel puțin 5000 fișiere unice pe ora în perioada de vârf și un total de 35000 de fișiere unice pe zi.
• Se va furniza o soluție de sine stătătoare pentru fiecare entitate care utilizează ECRIS Parchete (PICCJ, DNA și DIICOT)
• Fiecare set implementat la ECRIS Parchete va include cel puțin două echipamente de protecție avansată și componenta de management centralizat în centrul principal de date și un echipament și componenta de management pentru locația BCDR

7. Stocarea si accesul la documentele electronice.

Spre deosebire de metadate, documentele NU vor fi stocate într-o baza de date relațională. Pentru stocarea documentelor este recomandată fie stocarea documentelor pe sistemul de fișiere folosind o tehnologie integrată cu baza de date (Microsoft SQL Server FILESTREAM, Oracle BFILE sau echivalent) fie folosirea unei baze de date orientate pe documente/NoSQL (MongoDB+GridFS, HDFS, CouchDB sau echivalent).
La nivelul documentelor, operațiunile permise vor fi de adăugare, ștergere și adăugare versiune. Astfel conținutul unui fișier încărcat nu va putea fi modificat decât prin adăugarea unei versiuni în situațiile în care logica aplicației permite acest comportament.

IMPORTANT: Așa cum se observă în diagramă, bazele de date de documente nu aparțin unui tenant. Acest detaliu va permite referențierea unui document în cadrul aceluiași nod de către tenants diferiți, respectiv documentele vor fi partajate intre tenants la nivel tehnic. În cazul nodurilor multi-tenant, respectiv nodurile care găzduiesc datele mai multor instituții, cum este cazul nodului centralizat MJ sau în cazul celor trei instalări centralizate din cadrul parchetelor (PICCJ, DNA și DIICOT), există oportunitatea păstrării unei referințe unice la un document atunci când un document este folosit în mai multe dosare, fără ca acesta să fie duplicat. Acest caz este foarte comun în cazul căilor de atac când dosarul este transferat pentru apel/recurs la instanța superioară. La transferul dosarului toate documentele dosarului trebuie să ajungă și la instanța superioară. Întrucât ambele Instanțe sunt găzduite pe același nod duplicarea documentelor nu este necesară. Acest comportament este posibil

având în vedere că documentele nu se vor modifica, ci doar se vor versiona. Astfel referențierea versiunilor unui document este posibilă. Comportamentul de referențiere este esențial din motive de economie de spațiu.

7.1 Sistem de stocare si redare Video / Multimedia

Sistemul va asigura stocarea centralizată a înregistrărilor de audieri și a altor materiale video și audio depuse de parchete sau instantele de judecata în dosarul electronic de instanță. Documentele electronice din dosarul electronic al Instanței vor fi păstrate în bazele de date ale aplicației ECRIS Instanțe, cu excepția înregistrărilor video și audio. Acestea vor fi stocate centralizat per tenant.
Acest sistem va asigura pastrarea înregistrărilor audio și video și integrarea cu aplicația ECRIS. Sistemul trebuie să ofere posibilitatea de streaming video și audio, astfel încât un utilizator al aplicației ECRIS să poată accesa foarte ușor o înregistrare video sau audio, fără a fi nevoit să descarce integral fișierul pe calculatorul propriu.
Sistemul trebuie să asigure și transformarea (encoding) fișierelor multimedia într-un format potrivit pentru streaming multimedia (ex: H.264 sau H.265 preferabil datorită compresiei mai bune). Standardul de compresie va fi stabilit în perioada de implementare.

IMPORTANT: din motive legale, în cazul fișierelor video și audio ce vor fi convertite la un standard comun, sistemul va păstra și originalul. De asemenea sistemul trebuie să permită semnarea și marcarea temporară a conținutului pentru a se împiedica alterarea acestora.

NOTĂ: Sistemul video/multimedia este o extensie a dosarului electronic, astfel stocarea conținutului multimedia se poate face folosind același sistem de persistare al fișierelor ce urmează să fie folosit și pentru restul documentelor din dosarul electronic, cu deosebirea că pentru fișierele multimedia va fi necesară implementarea funcționalităților suplimentare descrise mai sus (encoding, streaming etc.).

8. Arhiva electronica

ECRIS este proiectat să conțină în dotarea sa un sistem de arhivare electronică a dosarelor soluționate. Acest sistem este menit și dimensionat să găzduiască un număr foarte mare de dosare pe perioade lungi de timp. Sistemul de arhivare are de asemenea o copie în nodul BCDR. Arhivarea dosarelor se face pe dispozitive de înalta performanță și sunt securizate astfel încât să nu poată fi modificate sau șterse din arhivă nici intenționat și nici din greșeala.
Arhiva este proiectată să fie dotată cu dispozitive de unica folosință în scriere, dar cu multiple utilizări în citire, aceata fiind descrisa mai sus. Cu ajutorul acestei tehnologii se asigura permanența și integritatea informațiilor arhivate, pe durate lungi de timp, iar dispozitivele ce stochează toate dosarele în format electronic, vor fi îndeajuns de flexibile încât să poată fi redimensionate la nevoie, fără să aibă nevoie de alte schimbări de infrastructură.
Aplicația de arhiva electronica va asigura arhivarea permanenta a informațiilor din aplicațiile sistemului ECRIS cu excepția aplicațiilor dedicate parchetelor care vor beneficia de o componenta de arhivare dedicata. Aplicația de arhivare va fi folosită de Instanțele de judecata, CSM, Inspecția Judiciară, Ministerul Justiției și instituțiile subordonate (ANABI, DNP). Informațiile arhivate vor fi stocate pe echipamente specializate tip WORM.
Arhiva electronică a parchetelor este similară cu arhiva electronică disponibilă în cadrul Instanțelor.
Arhivarea electronica a dosarelor din instante se va efectua in doua etape:logică și permnentă.

8.1 Arhivarea Logica

În cadrul sistemului ECRIS vor fi prevăzute două tipuri de arhivare: logică și permanentă. Arhivarea logică va păstra informațiile în sistemele de stocare online iar informațiile arhivate vor fi marcate logic ca fiind arhivate (flag de arhivare). Arhivarea permanentă va presupune transferarea efectivă a datelor în sisteme de arhivare dedicate cu caracteristici WORM.

IMPORTANT: pentru arhivarea logică datele vor fi păstrate în aceleași tabele și baze de date, dar vor fi marcate logic ca fiind arhivate, respectiv datele NU vor fi transferate în alte tabele sau baze de date dedicate arhivei logice. Transferul datelor arhivate logic în cadrul aceleiași baze de date generează în timp complexitate nenecesară care nu poate fi ușor controlată și din acest motiv această abordare NU este recomandată. Această abordare a fost folosită în ECRIS 4 și versiunile anterioare unde și-a dovedit ineficacitatea. Astfel datele arhivate logic vor fi păstrate în aceleași tabele cu datele nearhivate, iar filtrarea se va realiza prin intermediul unor structuri de tip view (recomandat) sau la nivel de logică de aplicație. Pentru aplicațiile care folosesc sharding, este recomandat ca datele arhivate să fie persistate în shard-uri dedicate arhivei logice pentru a descărca bazele de date online, cu condiția ca distribuirea să facă parte din strategia normală de sharding. Altfel spus este esențial ca datele arhivate logic să NU primească un tratament separat în logica aplicației (în afara eventualei filtrări logice), respectiv o interogare (query) care cuprinde atât date nearhivate cât și date arhivate logic nu trebuie să fie cu nimic diferită față de o interogare care cuprinde doar date nearhivate sau doar date arhivate. În eventualitatea în care datele arhivate sunt stocate în shard-uri separate, un astfel de query va fi rezolvat prin mecanismul general de interogare multi-shard, în mod transparent pentru componentele de logica ale aplicației.
Arhivarea dosarelor este o functionalitate comuna ECRIS Instante si ECRIS Parchete care permite degrevarea sistemului de acele dosare care au ieșit din perioada lor activa.
Aceasta functionalitate implementeaza politicile de arhivare definite in cadrul ECRIS si foloseste modelul de autorizare al ECRIS.
Dosarele sunt in esenta alcatuite din doua componente:
• Metadatele care sunt obiecte relationale salvate intr-o baza de date relationala si pot fi folosite inclusiv in operatii de cautare si regasire dosar.
• Documentele – care sunt obiecte semistructurate sau nestructurate (documente, scanuri, fisiere multimedia, etc.).
Solutia de arhivare logica va avea ca functionalitate:
• Marcarea metadatelor ca trebuie arhivate – lucru care va reduce aria de cautare în platformă – cautarea in mod normal va fi realizata in dosarele nearhivate, iar in mod explicit si in functie de permisiuni se pot cauta si dosarele arhivate.
Functii ale solutiei de arhivare:
• Definire politici de arhivare pe baza urmatoarelor criterii:
  - ✓ Obiect al dosarului
  - ✓ Perioada după care se arhivează
  - ✓ Tipul de decizie din dosar care declanșează calculul perioadei de arhivare
• Arhivarea este un proces batch care rulează conform configurărilor sistem (nu mai rar de 1 / săptămână).
• Căutarea în Arhivă folosește aceleași criterii de căutare – in cadrul metadatelor dosarului – ca si funcția de căutare în ECRIS.
• Vizualizarea dosarului arhivat:
  - ✓ Pentru metadate se face similar cu vizualizarea unui dosar nearhivat.

8.2 Arhivarea Permanenta:

Aplicația de arhivă electronică va asigura arhivarea permanenta a informațiilor din aplicațiile sistemului ECRIS cu excepția aplicațiilor dedicate parchetelor care vor beneficia de o componenta de arhivare dedicata. Informațiile arhivate vor fi stocate pe echipamente specializate tip WORM.
Vizualizarea dosarului arhivat permanent:

- ✓ Pentru documente trebuie initiata o procedura de restaurare a documentelor din arhiva. Utilizatorul va completa o cerere de aducere din arhiva a dosarelor (incluzând motivul) și va fi notificat în momentul în care acest proces este terminat. Aducea unui dosar din Arhivă este un proces asincron care trebuie să se termine in maxim 48h.

Ofertantul trebuie sa prezinte distinct in cadrul propunerii tehnice tehnologiile/produsele utilizate pentru indeplinirea cerintelor, modul in care acestea vor fi adaptate specificului cerintelor, eventalele constrangeri tehnologice, precum si durata si resursele alocate dezvoltarii acestei componente. In oferta financiara costurile dezvoltarii acestei componente trebuie evidentiate distinct.

9. Nomenclatoare

9.1 Reguli tehnice generale de realizare/actualizare (administrare) a nomenclatoarelor (daca exista)

Cerintele acestei componente vor fi detaliate in etapa de Analiza Detaliata.

9.2 Reguli tehnice generale de realizare/actualizare(administrare) a nomenclatoarelor comune Instante/Parchete

Cerintele acestei componente vor fi detaliate in etapa de Analiza Detaliata.

10. Rapoarte

Pentru raportare se vor folosi baze de date distincte, astfel încât interogările de raportare să nu afecteze performanța aplicațiilor principale. În funcțiile de cerințele de raportare ale aplicației, bazele de raportare pot fi replici OLTP peste care opțional se pot construi baze de date OLAP. Implementarea de baze de date OLAP este recomandată cel puțin pentru aplicațiile de Statistici, ECRIS Instanțe și ECRIS Parchete.
Rapoartele vor folosi un modul web generator de rapoarte/analize dinamice de tip „Report Builder" care va pune la dispoziția utilizatorului unelte specifice generării de rapoarte și analize în tehnologie „Drag&Drop" fără a necesita cunoştinţe tehnice IT din partea utilizatorului, precum și o unealtă de interogare și analiză front-end pentru bazele de date
Functionalitati ale modulului:
1. Va putea genera rapoarte de tip Pivot şi Cross-Tab direct din interfata Web;
2. Va conține un set de instrumente de tip grafice “Chart” predefinite care va conține cel puțin grafice de tip: Bar Chart, Line Chart, Pie Chart Scatter Chart
3. Va genera rapoarte de tip tabel
4. Să permită construcția și salvarea sabloanelor de interogare.
5. Să permită exportul rezultatelor unui raport în forma electronica (minim: csv, excel, pdf) cu asigurarea distribuirii (share-link) doar către anumiți utilizatori;
6. Să permită imprimarea rezultatelor rapoartelor.
7. Sa permita autentificarea cu componenta de tip SSO.

11. Integrari

Toate aplicațiile din sistemul ECRIS vor fi dezvoltate folosind principiul “API First”. Astfel, furnizorul va proiecta în primul rând interfețele programatice ale aplicațiilor (Application Programmatic Interface). Interfețele utilizator (front-end) vor utiliza funcțiile oferite de API și vor fi dezvoltate decuplat (decoupled) de logica de business a API-urilor. API-urile aplicațiilor din sistemul ECRIS vor fi singurul punct de acces la funcționalitatea sistemelor componente.
Acest principiu va asigura o integrabilitate ușoară a aplicațiilor din sistemul ECRIS cu alte aplicații. De asemenea respectarea acestui principiu va asigura un proces de proiectare detaliată mai riguros, cu respectarea principiilor arhitecturale enunțate mai jos și va reduce riscurile tehnice ale proiectului.
Integrările necesare sistemului ECRIS sunt enumerate în documentul „2.2.1.B – Integrări între sisteme” parte din livrabilul 2.2.1 – Cerințe non-funcționale. Prin integrare înțelegem interconectarea directă, la nivel tehnic, dintre două sisteme informatice cu scopul de a schimba informații relevante pentru ambele sisteme.
Integrările dintre aplicațiile sistemului ECRIS se împart în două categorii:
- Integrările dintre aplicațiile sistemului ECRIS .
- Integrări dintre aplicații ale sistemului ECRIS și aplicații externe.

Prin aplicație externă înțelegem orice aplicație ce nu face parte din scopul sistemului ECRIS, inclusiv aplicații operate de instituții din sistemul de justiție.
Toate integrările necesare sunt enumerate în documentul L2.2.1.B – Integrari intre sisteme.xlsx (sublivrabil al livrabilului 2.2.1 – Cerinte non-functionale).
Accesarea funcționalității ECRIS de către aplicații externe
Acest tip de integrare va fi rezolvată natural prin intermediul API-urilor expuse de aplicațiile ECRIS și API Gateway-urile Instanțelor și parchetelor.
Accesarea funcționalității aplicațiilor externe de către ECRIS
Acest tip de integrare va fi rezolvată de fiecare aplicație ECRIS ținând cont de specificul tehnic al integrării. În acest sens la nivelul de logică vor fi dezvoltate componente de tip conector (proxy) care vor împacheta detaliile tehnice ale integrării respectând regulile arhitecturale ECRIS (ex serializare, autentificare, samd.). Aceste componente reutilizabile vor fi ulterior folosite în cadrul aplicațiilor pentru implementarea integrărilor. Dezvoltarea unei librării de astfel de conectori reutilizabili va reduce efortul de dezvoltare și va asigura o abordare consistentă a integrărilor.

11.1 Integrări între aplicațiile sistemului ECRIS

Toate integrările dintre aplicațiile sistemului ECRIS sunt în scopul sistemului ECRIS și vor fi dezvoltate în cadrul proiectului. Din punct de vedere tehnic aceste integrări vor fi dezvoltate folosind API-urile fiecărei aplicații ECRIS.
Un exemplu de integrare importantă este integrarea dintre aplicația ECRIS Parchete și ECRIS Instanțe. Aceasta integrare va asigura câteva funcționalități importante cum ar fi:

- Inițierea unui dosar penal nou pe rolul Instanțelor direct din aplicația ECRIS Parchete.
- Evidența dosarelor penale aflate pe rolul Instanțelor.
- Interacțiunea în cadrul unui dosar penal și instanța de judecată.
- etc.

În exemplul de mai sus, integrarea va fi realizată folosind API Gateway-ul Instanțelor, respectiv în cadrul aplicației ECRIS Parchete vor fi dezvoltate componente de logică care vor apela API Gateway-ul Instanțelor pentru a implementa funcționalitatea cerută.

Cerințele funcționale pentru integrările dintre aplicațiile sistemului ECRIS sunt descrise în documentele de cerințe funcționale ale fiecărei aplicații.

11.2 Integrări dintre aplicațiile sistemului ECRIS și aplicații externe

În privința integrărilor dintre aplicațiile ECRIS și alte aplicații există mai multe opțiuni de implementare în funcție de specificul fiecărei aplicații externe și specificul integrării.

11.3 API (inclusiv UI)

11.3.1 Concepte generale privind API

Din punct de vedere conceptual componenta API este situată în cadrul nivelului de prezentare. Cu toate acestea din punct de vedere al împachetării (packing) aceasta va fi cuplată cu nivelul de logică.
Componenta API va fi implementată folosind o arhitectură de tip REST și formatare JSON. API-ul va implementa un standard REST, spre exemplu OData (recomandat), ORDS sau echivalent.
Componenta API a oricărei aplicații va fi documentată folosind un standard de documentare tip Swagger sau echivalent. Documentația API va fi publicată online, iar accesul la documentație va fi disponibil în funcție de politica fiecărei instituții. Este recomandat ca documentația API să fie disponibilă public, indiferent de restricțiile aplicate pentru accesul la API. În acest fel se vor facilita integrările cu diversele aplicații externe.
IMPORTANT: la nivel european există inițiativa European Interoperability Framework de definire a unor standarde de interoperabilitate pentru sistemele administrației publice. O componentă importantă a EIF este ISA2 (https://ec.europa.eu/isa2/isa2_en) – "Interoperability solutions for public administrations, businesses and citizens". Dezvoltarea API-urilor ECRIS trebuie să fie aliniată cu eforturile europene de interoperabilitate și standardizare. În acest sens în faza inițială a proiectului de implementare se va evalua progresul ISA2 și/sau alte inițiative de standardizare la nivel european. La momentul elaborării documentului de arhitectura ISA2 definește câteva soluții reutilizabile. Dintre acestea soluția de Core Vocabularies (vocabular comun) definește câteva scheme reutilizabile de entități, cum ar fi Persoană, Agent, Adresă, Organizație publică, Document etc. Desigur aceste concepte nu acoperă necesitățile ECRIS, totuși pot fi aplicate în modelarea domeniului pentru ECRIS V, astfel încât alinierea la un standard european comun de interoperabilitate să poată fi realizată mai ușor
Tehnologii candidat

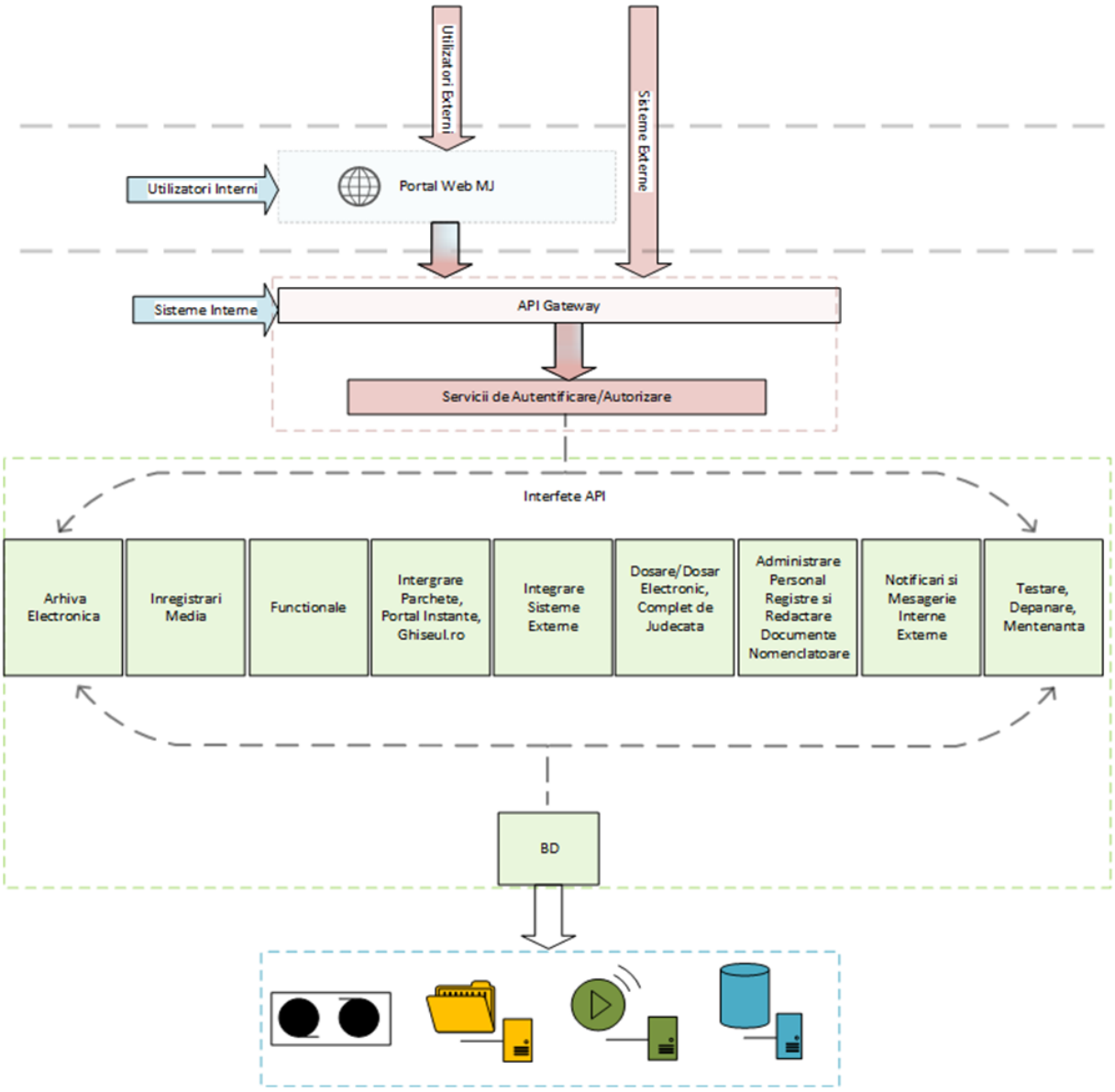
- **Standard API**: OData, ORDS sau echivalent + ISA2 sau versiuni viitoare
- **Documentare API**: Swagger sau echivalent

11.3.2 Componentele Principale ale API

Nivelul acesta joaca rol de interfața de legătura și control între cel de Prezentare, funcționalitățile și bazele de date ECRIS. La acest nivel se definesc API-urile de acces în sistem, validarea sau invalidarea utilizatorilor și implementează unul din nivelele de securitate ale sistemului (API Gateway). Aici sunt validați atât utilizatorii ce ajung prin intermediul portalului de mai sus cât și utilizatorii automați (alte sisteme) atât din exterior (cum ar fi de exemplu integrarea cu Politia de Frontiera) cât și cei considerați ca fiind parte din sistemul ECRIS însă sunt externi implementării particulare MJ sau Parchete.
Componentele acestui nivel sunt următoarele:

- API validare și conectare utilizatori interni
- API validare și conectare utilizatori externi

- API validare și conectare sisteme interne
- API validare și conectare sisteme externe
- API de legătură cu funcționalitățile de logică ECRIS
- API Arhiva Electronică
- API Înregistrări Media
- API Integrare Parchete, Portal Instanțe, Ghișeul.ro (Interne)
- API Integrare Sisteme Externe
- API Dosare și Complet Judecată
- API Administrare Personal, Registre, Redactare Documente și Nomenclatoare
- API Notificări și Mesagerie Diversă
- API de Testare, Depanare, Mentenanță
- API BD



11.3.3 Securizarea accesului la date prin API

Sistemul va permite accesul securizat la date prin API, astfel încât să se respecte mecanismele de autorizare specifice implementate în aplicație. Un utilizator nu va avea acces la date prin API mai mult decât este definit la nivelul rolului de securitate.

11.3.4 Compatibilitate API-uri cu tehnologii standard

Sistemul trebuie să expună interfețe programabile (API) care să adere la tehnologii standard, cum ar fi OData, ORDS, gRPC, REST, etc, pentru a permite o integrare facilă a componentelor sistemului.

11.3.5 Catalog online API-uri cu tehnologii standard

Sistemul trebuie să expună un catalog online pentru toate interfețele programabile (API) expuse, cu descrierea funcționalităților și a metodelor expuse. Catalogul va include documentație în format standard (ex: Swagger) pentru fiecare metodă disponibilă din interfețele programabile.

11.4 API Gateway

11.4.1 API Gateway Instanțe

În mod similar portalului, componenta API Gateway a Instanțelor va fi punctul unic de interacțiune dintre alte aplicații și ECRIS Instanțe. Aceasta este componenta cheie pentru integrarea facila a sistemului ECRIS cu alte sisteme.
API Gateway va agrega toate API-urile disponibile la nivelul Instanțelor și va redirecționa apelurile către API-ul corespunzător. De asemenea API Gateway va asigura accesul securizat, autentificând și autorizând apelanții.
Așa cum este menționat mai sus, portalul instanțelor va utiliza componenta API Gateway. Din acest punct de vedere portalul trebuie privit ca orice alta aplicație terță care se integrează cu ECRIS Instanțe.
Integrarea dintre celelalte aplicații ale sistemului de justiție și ECRIS Instanțe se va face prin API Gateway. în mod special integrarea dintre ECRIS Parchete și ECRIS Instanțe se va realiza prin componentele API gateway ale celor doua aplicații. Trebuie subliniat faptul ca toate integrările între alte aplicații și ECRIS Instanțe vor fi realizate prin API Gateway. Spre exemplu o integrarea la nivel de baze de date, intre ECRIS Instanțe și ECRIS Parchete nu este permisă.
Aceasta componentă va permite extinderea facilă a sistemului ECRIS cu alte aplicații, inclusiv aplicații dezvoltate de terți. Spre exemplu ne putem imagina furnizori externi care dezvolta aplicații dedicate avocaților pentru managementul dosarelor. Ne putem imagina aplicații mobile, dezvoltate de sistemul de justiție sau de furnizori terți, pentru accesul la informațiile din dosar. Ne putem chiar imagina în viitor o piață deschisă de aplicații (in genul Apple Store/Google Marketplace) pentru aplicații specifice sistemului de justiție.

11.4.2 API Gateway parchete

Componenta API gateway pentru parchete este similară componentei API Gateway Instanțe.

11.5 Hub Integrare

Ca alternativă pentru integrările directe, sistemul ECRIS va dispune și de HUB-ul de integrare (descris în acest document) care va oferi o alternativă mai rapidă pentru integrări cu alte instituții, inclusiv în cazul în care instituțiile respective nu dispun de un sistem informatic ce poate fi integrat.

Acest sistem generic va asigura o opțiune alternativă pentru integrarea aplicațiilor din sistemul ECRIS cu alte sisteme externe sistemului ECRIS. Într-un scenariu ideal toate integrările cu sistemele externe se vor realiza prin integrări directe între sisteme. Acest tip de integrări sistem cu system, va presupune însă costuri și o durată mare de implementare, timp în care lipsa integrărilor va afecta eficiența tuturor instituțiilor implicate. De asemenea aceste integrări depind foarte mult de caracteristicile tehnice ale sistemelor ce trebuie integrate și, evident, de existența unor astfel de sisteme. Ținând cont de aceste constrângeri, HUB-ul de integrare propune o soluție alternativă la problematica integrărilor.
Este important de subliniat că acest hub nu va fi folosit pentru dezvoltarea integrărilor dintre aplicațiile sistemului ECRIS (acestea vor fi directe) și nici nu își propune să înlocuiască integrările directe, ci va oferi o opțiune rapidă și simplă pentru integrarea cu alte sisteme, în lipsa altor variante. Eventual HUB-ul poate fi folosit temporar pentru diverse integrări intre instituții, până când o integrare directă este implementată.
Câteva exemple de utilizare ar fi următoarele:
• integrarea dintre sistemul ECRIS Instanțe și sistemul folosit de Uniunea Națională a Executorilor Judecătorești;
• integrarea dintre ECRIS Parchete și sistemul bancar;
• integrarea dintre ANP și DNP;
• șamd.
Utilizatorii acestui sistem vor fi instituții înregistrate, cu drepturi și permisiuni de securitate bine definite. Sistemul va expune atât o interfață utilizator cât și un API propriu, astfel instituțiile vor putea accesa sistemul folosind fie interfața utilizator, fie vor putea integra sistemele proprii cu acest sistem (via API).
Prin acest sistem fiecare instituție va putea genera evenimente și va putea consuma evenimente. Spre exemplu ANP ar putea genera un eveniment la liberarea unei persoane, iar DNP va consuma acest eveniment. În mod similar și alte instituții ar putea consuma evenimentul de liberare dacă este relevant. Prin eveniment se înțelege un set de informații structurate și o colecție de documente. În cazul ANP, evenimentul de liberare ar putea conține informații despre persoana liberată și documentul de liberare.
ANP va putea genera acest eveniment fie prin interfața utilizator a aplicației, respectiv un utilizator al ANP va genera manual evenimentul completând datele în sistem sau prin integrarea dintre sistemul de evidență al ANP cu API-ul Hub-ului de integrare. În mod similar DNP va putea consuma evenimentul accesând interfața utilizator a Hub-ului, respectiv un utilizator din registratura DNP va procesa evenimentul de la ANP, sau printr-o integrare dintre sistemul DNP și API-ul hub-ului de integrare. În ambele situații niciuna dintre instituții nu va fi preocupată de detaliile tehnice de implementare ale celeilalte instituții. Mai mult „integrarea” între instituții va fi posibila chiar dacă una dintre instituții nu dispune de un sistem informatic.
Exemplul de integrare dintre ANP și DNP este o cerință cunoscută de integrare și trebuie tratat doar ca un exemplu relevant. Cel mai probabil integrarea dintre ANP și DNP se va realiza prin integrarea directă a sistemelor, având în vedere că ambele instituții se află în subordinea Ministerului Justiției.

11.6 Hub Notificari

Componenta va centraliza mecanismele de transmitere a notificărilor astfel încât eventualele modificări ale mecanismelor de notificare să nu presupună modificări la nivelul tuturor aplicațiilor. În acest fel toate email-urile trimise de aplicațiile din sistemul ECRIS vor fi transmise centralizat fără a fi necesar ca în cadrul fiecărei aplicații să se implementeze un sistem distinct de notificare.
Acest sistem va permite schimbarea canalelor de transmitere și eventual chiar folosirea unor servere externe (gen MailChimp sau similar). De asemenea sistemul va permite în viitor și extinderea canalelor de notificare, spre exemplu prin adăugarea de notificări push care se transmit pe dispozitivele mobile ale utilizatorilor înregistrați. HUB-ul de notificări este o componentă tehnică

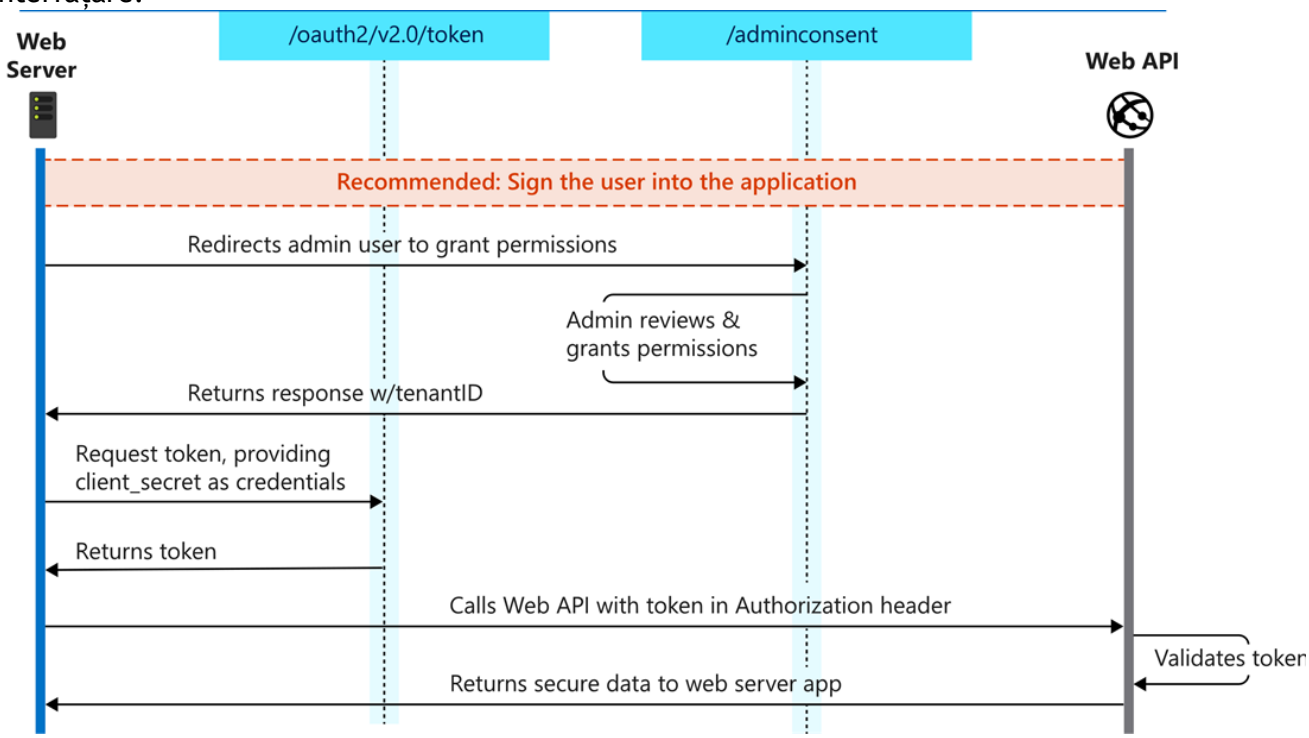
reutilizabilă sau subsistem distinct care va fi utilizată de fiecare aplicație sau instanțiată în cadrul fiecărui centru de date (MJ, PICCJ, DNA, DIICOT).

11.7 Detalii tehnice de implementare servicii web

Interfațarea dintre aplicațiile ECRIS Instanțe si ANABI va folosi doua tipuri de interfețe programatice:

- interfețe funcționale care satisfac cerințele prezentate mai sus
- interfețe suport folosite pentru re-concilierea nomenclatoarelor comune folosite de sistemele integrate

Toate interfețele vor fi de tip Web API. Protocolul de transport este HTTPS.
Standardul de autentificare este bazat pe fluxul OAuth2 client credentials flow. Un exemplu este furnizat in diagrama de mai jos, in care Web Server este aplicația care apelează API-urile de interfațare.



Payload-urile transmise vor fi bazate pe un model de date agreat de comun acord si vor conține acolo unde este posibil cheile de business asociate nomenclatoarelor din sistemul țintă.

11.8 Lista de integrari posibile

Integrările necesare sistemului ECRIS sunt enumerate în documentul „2.2.1.B – Integrări între sisteme" parte din livrabilul 2.2.1 – Cerințe non-funcționale. Prin integrare înțelegem interconectarea directă, la nivel tehnic, dintre două sisteme informatice cu scopul de a schimba informații relevante pentru ambele sisteme.
Integrările dintre aplicațiile sistemului ECRIS se împart în două categorii:

- Integrările dintre aplicațiile sistemului ECRIS .
- Integrări dintre aplicații ale sistemului ECRIS și aplicații externe.

Prin aplicație externă înțelegem orice aplicație ce nu face parte din scopul sistemului ECRIS, inclusiv aplicații operate de instituții din sistemul de justiție.
Toate integrările necesare sunt enumerate în documentul ***L2.2.1.B - Integrari intre sisteme.xlsx*** (sublivrabil al livrabilului 2.2.1 – Cerinte non-functionale).

Fiecare integrare din lista de integrări este încadrată într-una dintre categorii: În scop sau Posibilă. Integrările în scop fac parte din scopul dezvoltării și vor fi implementate în cadrul proiectului.
Integrările posibile vor fi reanalizate înainte de lansarea procedurii de achiziție publică pentru implementarea ECRIS 5 și vor fi încadrate în categoria în scop, în funcție de prioritățile de la momentul respectiv și de fezabilitatea implementării integrărilor respective.
În etapa de analiza detaliata aceasta listă va fi revizuita, iar integrarile vor fi prioritizate conform metodei MOSCOW.

12. Portaluri

În cadrul sistemului ECRIS V exista mai multe portaluri, acestea avand atat componente publice cat si exclusive interne (exclusive pentru anumite categorii de personal din cadrul MJ, MP, CSM, ICCJ). Din acest motiv componentele de integrare cu aceste portaluri sunt unele complexe atat din punct de vedere tehnologic cat si din punct de vedere al securitatii accesului si transferului datelor. Cele mai importante portaluri, dar fara a ne rezuma la acestea sunt:

12.1 Cerinte generale

12.1.1 Cerinte tehnice generale

12.1.1.1 Operațiile de citire în cadrul portalului

Portalul Instanțelor va oferi funcționalități de consultare disponibile atât publicului larg (utilizatori anonimi) cât și persoanelor implicate într-un dosar (avocați, părți, procurori etc). Pentru aceste operații, API Gateway-ul (și implicit Portalul Instanțelor) va folosi o bază de date locală (cache) în care vor fi stocate temporar informațiile necesare.
La nivelul portalului va exista un index cu toate dosarele din sistem și un minim de metadate asociate. Acest index va fi folosit pentru implementarea funcției de căutare în cadrul portalului. În afara acestui index, restul de informații disponibile pe portal vor fi stocate temporar în baza de date cache a portalului.
Informațiile din cache vor fi populate pe măsură ce acestea sunt solicitate de utilizatori. Spre exemplu atunci când un utilizator accesează detaliile unui dosar, nodul central va apela nodul unde informațiile sunt persistate și va popula baza cache. Cache-ul va fi curățat în funcție de diverse politici, spre exemplu dosarele care nu au mai fost accesate în ultima luna vor fi șterse din cache, sau cache-ul va putea fi curățat periodic în fiecare săptămâna etc. Aceste politici vor fi stabilite în faza de design detaliat.
Pentru limitarea traficului către noduri, generat de portal, cache-ul va putea fi de asemenea actualizat și în perioadele cu utilizare mică (spre exemplu noaptea).
Anumite operații efectuate la nivelul Instanțelor vor putea de asemenea invalida anumite obiecte din cache și eventual chiar forța o reactualizare. Spre exemplu, adăugarea unui nou termen de judecată ar putea genera o actualizarea a informațiilor dosarului în baza cache.

12.1.1.2 Operațiile de modificare în cadrul portalului

Portalul Instanțelor va oferi de asemenea funcționalități interactive, spre exemplu depunerea de documente în cadrul dosarului sau solicitarea unei amânări etc. Aceste operații de modificare vor putea fi realizate de utilizatori prin intermediul Portalului. Aceleași operații vor putea fi realizate și

de alte sisteme prin intermediul API Gateway. Un exemplu este integrarea dintre ECRIS Parchete și ECRIS Instanțe care va fi realizată prin intermediul API Gateway Instanțe.
Operațiile de modificare vor fi stocate de API Gateway într-o coada de mesaje specifica fiecărei Instanțe de judecată (tenant). Un istoric al acestor mesaje va fi de asemenea stocat în baza centrală, în special pentru a putea fi vizualizate în cadrul portalului. Mesajele din coadă vor fi consumate de componenta de sincronizare disponibilă în cadrul fiecărui nod care va apela API-ul nodului și va executa operația de modificare la nivelul nodului, indicând nodului central aplicarea cu succes a modificării, respectiv modificarea statusului operației.
Utilizarea unor mecanisme de tip coada pentru comunicare este necesară pentru a garanta livrarea mesajelor în scenarii în care nodul țintă nu este online și în același timp, pentru a implementa un mecanism asincron de comunicare. Utilizarea cozilor permite inclusiv temporizarea componentei de sincronizare. De exemplu, componenta de sincronizare ar putea fi activă doar în perioadele cu utilizare redusă sau ar putea ține cont de încărcarea generală a sistemului.

12.1.1.3 Operațiile de căutare

Pentru implementarea operațiilor de căutare la nivelul portalului se va folosi un catalog de căutare (index) construit pe baza informațiilor din catalogul global de obiecte.

12.1.1.4 Independența de locația fizică

Portalurile publice ale sistemului trebuie să permită accesul indiferent de punctul fizic de acces, pe baza drepturilor/rolurilor stabilite la logarea în sistem.

12.1.1.5 Optimizarea în funcție de dispozitiv

Portalurile publice ale sistemului trebuie să optimizeze automat interfața (formatul elementelor, organizarea informației etc) în funcție de dispozitivul de pe care este accesată aplicația și rezoluția acestuia: PC, laptop, tabletă.

12.1.2 Cerinte de Securitate generale

12.1.2.1 Evaluarea portaluri ECRIS

În plus față de testul volumetric menționat anterior, ce are ca scop principal evaluarea infrastructurii, se va realiza un test de performanță cu focus principal pe modulele aplicației astfel încât să fie evaluate performanțele individuale la nivelul portalului ECRIS.
Acest test evaluează modul în care funcționează portalul ECRIS în ceea ce privește capacitatea de reacție și stabilitatea într-un anumit volum de lucru. De asemenea, servește la investigarea, măsurarea, validarea sau verificarea altor atribute de calitate ale sistemului, cum ar fi scalabilitatea, fiabilitatea și utilizarea resurselor în ceea ce privește timpul de procesare și rata de transfer etc. În cadrul acestui test avem tipuri de teste de performanță, care sunt descrise mai jos.

- Testarea încărcării - evaluează comportamentul unei componente sau al portalului în ansamblu cu o sarcină în creștere, de exemplu numărul de utilizatori paraleli și/sau numărul de acțiuni, pentru a determina ce sarcină poate fi gestionată eficient de componenta analizată.
- Testarea de stres – evaluează portalul ECRIS sau o componentă a sa la limită sau dincolo de limitele sarcinilor sale de lucru anticipate sau specificate sau cu o disponibilitate redusă a resurselor (de exemplu: cu un server de prezentare oprit sau cu un singur nod de DB).

- Testarea volumetrică – evaluează comportamentul unei componente sau al portalului supus unor volume mari de date.

Acest test de performanță trebuie automatizat prin intermediul unor instrumente software și trebuie să urmărească efectuarea unor fluxuri de business complete (end-to-end) simulând acțiunea utilizatorilor.
Numărul utilizatorilor simulați și fluxurile de lucru simulate vor fi detaliate de către beneficiar în momentul realizării testelor.
Vor fi testate individual performanțele tuturor portalurilor ECRIS ce furnizează servicii funcționale către utilizatori.
Raportul detaliat al rezultatului de testare de performanță pentru portalul ECRIS este parte din livrabilele de proiect.

12.2 Portal Instante

Portalul Instanțelor este componenta cheie pentru digitalizarea sistemului de justiție. Portalul instanțelor este aplicația care va fi folosită de terți – părțile unui dosar, avocați și alți terți interesați - în relație cu Instanțele din România. Portalul va fi punctul unic pentru interacțiunea online dintre cetățeni și Instanțele din România. Portalul instanțelor va deservi toate instanțele de judecată și va oferi și funcționalități de tip Content Management System, care vor permite instanțelor să își administreze propriile pagini de prezentare (date de contact, comunicări șamd).
În versiunea curentă a sistemului, există portalul Instanțelor de judecată (https://portal.just.ro) care conține site-urile Instanțelor de judecată din România și printre altele prezintă spre consultare și informațiile publice despre dosarele aflate pe rolul Instanțelor și ședințele de judecată. De asemenea există site-ul web al ÎCCJ, respectiv www.scj.ro care de asemenea permite consultarea dosarelor cu anumite detalii suplimentare specifice ICCJ. Funcționalitățile de consultare ale celor două portaluri vor fi unificate și vor fi în continuare disponibile și în noua versiune a sistemului.
Informațiile publice vor fi în continuare accesibile pentru publicul larg (fără a fi necesară autentificare).
Suplimentar, în noua versiune a portalului, va exista și o secțiune autorizată prin care utilizatorii autorizați pot interacționa online cu Instanțele. Spre exemplu, prin intermediul acestei secțiuni a portalului, avocații vor depune documente online (inclusiv semnate electronic), fără a fi nevoiți să se deplaseze la instanță. De asemenea, părțile unui dosar vor putea consulta conținutul unui dosar.
Portalul Instanțelor va utiliza funcțiile oferite de gateway, respectiv portalul va expune funcționalitatea oferită de componenta API gateway sub forma unei interfețe utilizator. În acest sens portalul va fi strict o interfață utilizator (front-end) și nu va implementa logica proprie, toate funcțiile necesare fiind implementate la nivelul API Gateway.

12.2.1 Cerinte tehnice specifice

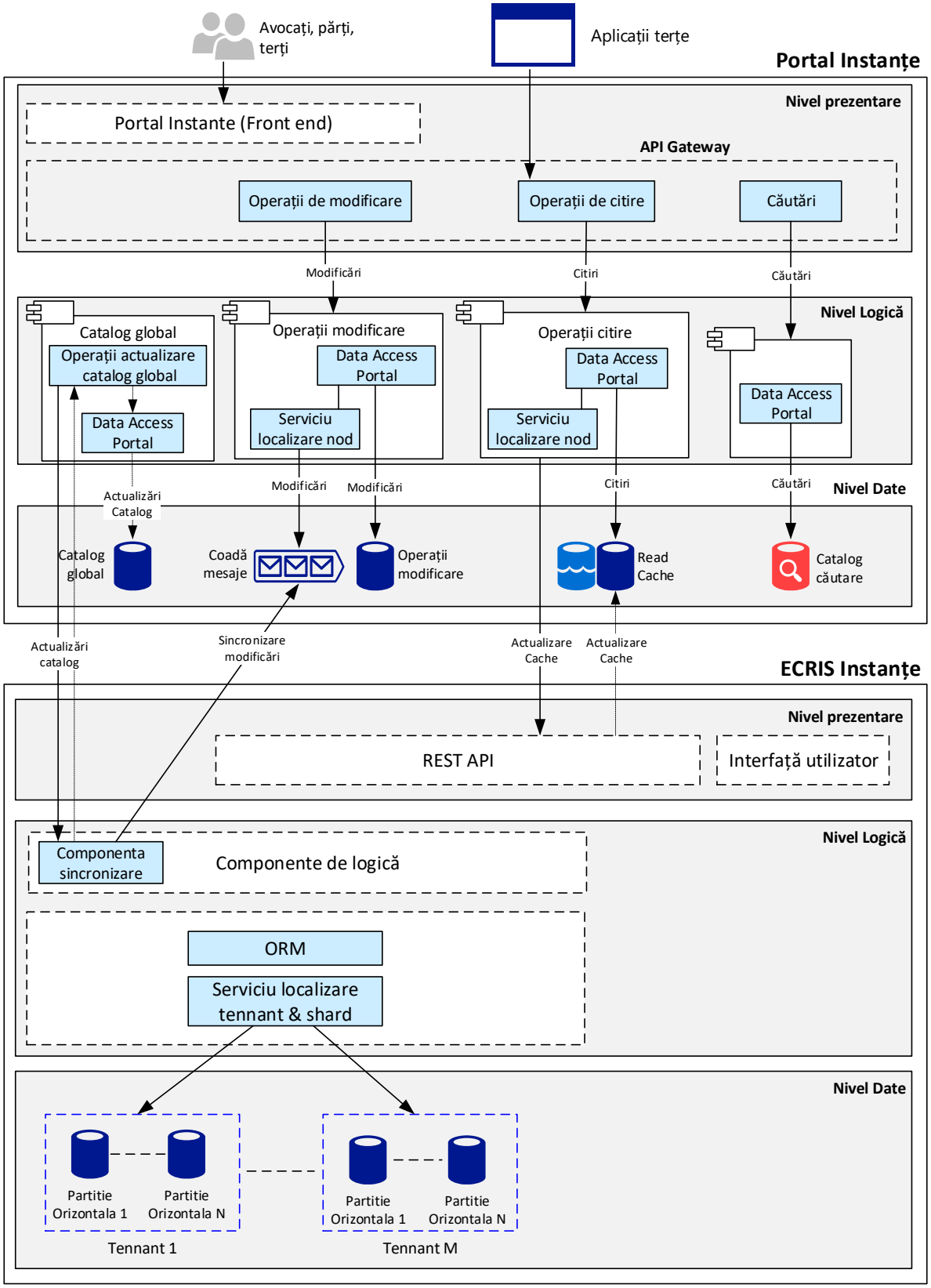
12.2.1.1 Distribuția și localizarea informațiilor Instanțelor

Informațiile legate de dosarele de judecată reprezintă majoritatea informațiilor ce vor fi stocate în bazele de date ale aplicației ECRIS Instanțe, aplicație care va fi instalată pe un nod central, într-o arhitectură virtualizată alcătuită din mai multe noduri virtuale. La un moment de timp un dosar se află pe rolul unei singure Instanțe de judecată și toate informațiile legate de un dosar se află în contextul acelui dosar, având puține relații externe, fapt ce permite distribuirea dosarului și a informațiilor asociate pe mai multe noduri fizice și în mai multe baze de date și partiții orizontale (sharding) cu consecințe rezonabile asupra complexității întregului sistem și beneficii considerabile în privința performanței și a scalabilității.

Având în vedere distribuția datelor pe mai multe noduri este foarte important ca în orice moment să fie cunoscută sursa principală a datelor (single truth). Ca **regulă general aplicabilă toate informațiile legate de dosarele de judecată vor fi stocate în bazele de date ale aplicației ECRIS Instanțe (metadate și documente)**.

În baza de date a portalului va exista doar o clonă a informațiilor pentru citire (cache) ce va fi actualizată în funcție de diferite politice de actualizare. De asemenea în baza de date a portalului va fi păstrat un istoric al operațiilor externe realizate de utilizatori (ex: depunerea unui nou document electronic).

În imaginea de mai jos este prezentată conceptual integrarea dintre Portalul Instanțelor și aplicația ECRIS Instanțe.



Figură 3 - integrarea dintre ECRIS Instanțe și Portal Instanțe

Pentru distribuirea datelor pe noduri, tenant și partiții este necesar ca la nivelul fiecărui obiect persistat în sistem să se cunoască locația acestuia. În acest sens la nivelul API Gateway va fi implementat un serviciu care va determina nodul pe care se află un anumit obiect. Pentru acest

serviciu se va implementa un catalog global de obiecte care va indica nodul de stocare. Acest catalog este de asemenea necesar pentru implementarea funcțiilor de căutare globale, astfel pe lângă locația fiecărui obiect (nod/tenant) catalogul va conține și metadatele necesare pentru implementarea căutărilor.
La nivelul fiecărui nod, la nivel de Data Access se va folosi o componentă similară pentru localizarea tenant-ului și a shard-ului în care obiectul se află. Strategia de sharding va fi stabilită în faza de design detaliat, existând multiple posibilități precum distribuirea în funcție de anul dosarului (un shard va stoca unul sau mai mulți ani), caz în care strategia de sharding poate fi de asemenea statică pe baza anului dosarului.

IMPORTANT: serviciul de localizare a unei partiții/shard este prezentat conceptual în documentul de arhitectură, însă în faza de design detaliat, este foarte recomandată utilizarea unor tehnologii existente și/sau facilități oferite de sistemul de baze de date folosit pentru implementarea sistemului, spre exemplu Elastic Database Client Library, Oracle Sharding/RAC sau tehnologii echivalente. NU este recomandată implementarea logicii de sharding la nivelul aplicației. Această recomandare nu se referă la serviciul de localizare a nodurilor pentru care este necesară implementarea la nivelul API Gateway.

12.2.1.2 Interogări multishard

O provocare a unui sistem care folosește sharding o constituie interogările multishard, respectiv interogări care returnează informații din mai multe shard-uri. Acestea nu pot fi complet evitate, însă pot fi reduse la design-ul detaliat prin design-ul API-ului și al interfeței utilizator. În cadrul unui tenant interogările multishard vor fi rezolvate la nivelul componentelor data acces.

12.2.1.3 Comunicarea inter-tenant

Există multiple funcționalități pentru care este necesară comunicare între doua Instanțe de judecată (tenants) aflate pe același nod (inter-tenant). Un bun exemplu ar fi transferul unui dosar la altă instanță în cazul căilor de atac.
Pentru aceste cazuri, comunicarea inter-tenant (între Instanțele de judecata) va fi rezolvată la nivelul componentelor de business logic sau via API-ul nodului,

12.2.1.4 Operații de actualizare a catalogului global de obiecte

Actualizarea catalogului global de obiecte se va face prin intermediul unei componente de logică implementate în API Gateway. Această componentă va sonda la anumite perioade de timp toate nodurile pentru a actualiza catalogul global cu obiectele noi și modificate. La nivelul nodului, se va implementa logică care va indica obiectele modificate (spre exemplu, prin folosirea de timestamps). Componenta de sincronizare va implementa o logică care va determina obiectele modificate (spre exemplu de la ultimul apel al nodului central).
Având în vedere că metadatele disponibile pentru căutare reprezintă un set redus de metadate (număr dosar, părțile, hotărârile pe scurt etc) controlul modificărilor nu presupune o complexitate foarte mare.
Pentru siguranță este necesar și un mecanism de reconstruire a catalogului global. Un astfel de mecanism va fi necesar pentru a putea repara eventualele inconsistențe care apar între catalogul global și noduri. De asemenea, mecanismul de reconstruire va fi necesar în cazul mutării anumitor tenants de pe un nod pe altul.

12.2.1.5 Structura bazelor de date API Gateway

În diagramă sunt folosite în scop ilustrativ mai multe pictograme de baze de date: catalogul global de obiecte, baza de date cu operații de modificare și read cache. Din punct de vedere al implementării aceste informații pot fi parte a aceleiași baze de date. Astfel catalogul global de obiecte poate fi implementat folosind o tabelă principală de dosare care pe lângă metadatele principale va avea asociată și informația localizării obiectului (nod/tenant). Read cache-ul și log-ul operațiilor de modificare pot fi implementate folosind tabele asociate aceluiași tabel principal. În timp ce catalogul global și operațiile de modificare vor fi persistate permanent, informațiile din "read cache" și documentele vor putea fi curățate conform politicilor de cache implementate la nivelul fiecărei aplicații.
Pentru implementarea acestor baze de date este recomandată partiționarea în mai multe shard-uri.

12.2.2 Cerinte functionale specifice

Cerintele functionale specifice portalului Instantelor se regasesc in cadrul livrabilului L2 - Portal Instante - Specificatii functionale.pdf
Portalul Ecris Intante trebuie sa ofere posibilitatea transmiterii live a sedintelor din dosarele civile (*http://legislatie.just.ro/Public/DetaliiDocument/241925*)

12.2.2.1 Informații volumetrice

In tabelul de mai jos sunt sintetizate câteva informații relevante pentru o privire de ansamblu.

Parametru	**Valoare**
Parametri generali	
Dimensiune stocare / pagina document (MB)	**0.125**
Instanțe	
Utilizatori interni (total angajați din schema de personal)	**12,781**
Nr de request-uri externe / zi. Estimarea se bazează pe traficul actual al portalului Instanțelor înmulțit cu 3, având în vedere ca noul portal va permite și interacțiunea online	**3,000,000**
Medie de dosare noi în fiecare an	**2,117,796**
Cauze soluționate anual	**2,170,715**

12.3 Portal Parchete

Portalul Parchetelor este de asemenea o componentă cheie pentru digitalizarea sistemului de justiție. Portalul Parchetelor este aplicația care va fi folosită de terți – suspecți, avocați - în relație cu parchetele din România. Portalul va fi punctul unic pentru interacțiunea online dintre cetățeni și parchetele din România.
În prezent, în cazul parchetelor nu există un portal echivalent portalului Instanțelor (https://portal.just.ro), respectiv componenta de portal a parchetelor este o componentă complet nouă.
Portalul Parchetelor va utiliza funcțiile oferite de gateway, respectiv portalul va expune funcționalitatea oferită de componenta API gateway sub forma unei interfețe utilizator. În acest sens

portalul va fi strict o interfață utilizator (front-end) și nu va implementa logica proprie, toate funcțiile necesare fiind implementate la nivelul API Gateway.

12.3.1 Arhitectura software ECRIS Parchete și Portal Parchete

Ca și în cazul Instantelor de judecată, aplicația ECRIS Parchete va fi instalată centralizat, pentru fiecare dintre cei trei tenants. Vor exista astfel trei instalări distincte:

- O instalare centralizată care va deservi Parchetul de pe lângă Înalta Curte de Casație și Justiție și parchetele subordonate.
- O instalare centralizată care va deservi Direcția Națională Anticorupție.
- O instalare centralizată care va deservi Direcția de Investigare a Infracțiunilor de Criminalitate Organizată și Terorism.

Este important de subliniat că cele trei instalări ale parchetelor vor fi complet separate. Diagrama prezintă instalarea care va deservi PÎCCJ. Instalările pentru DNA și DIICOT sunt identice, cu excepția echipamentelor hardware care vor fi diferite în funcție de necesitățile fiecărei instituții.

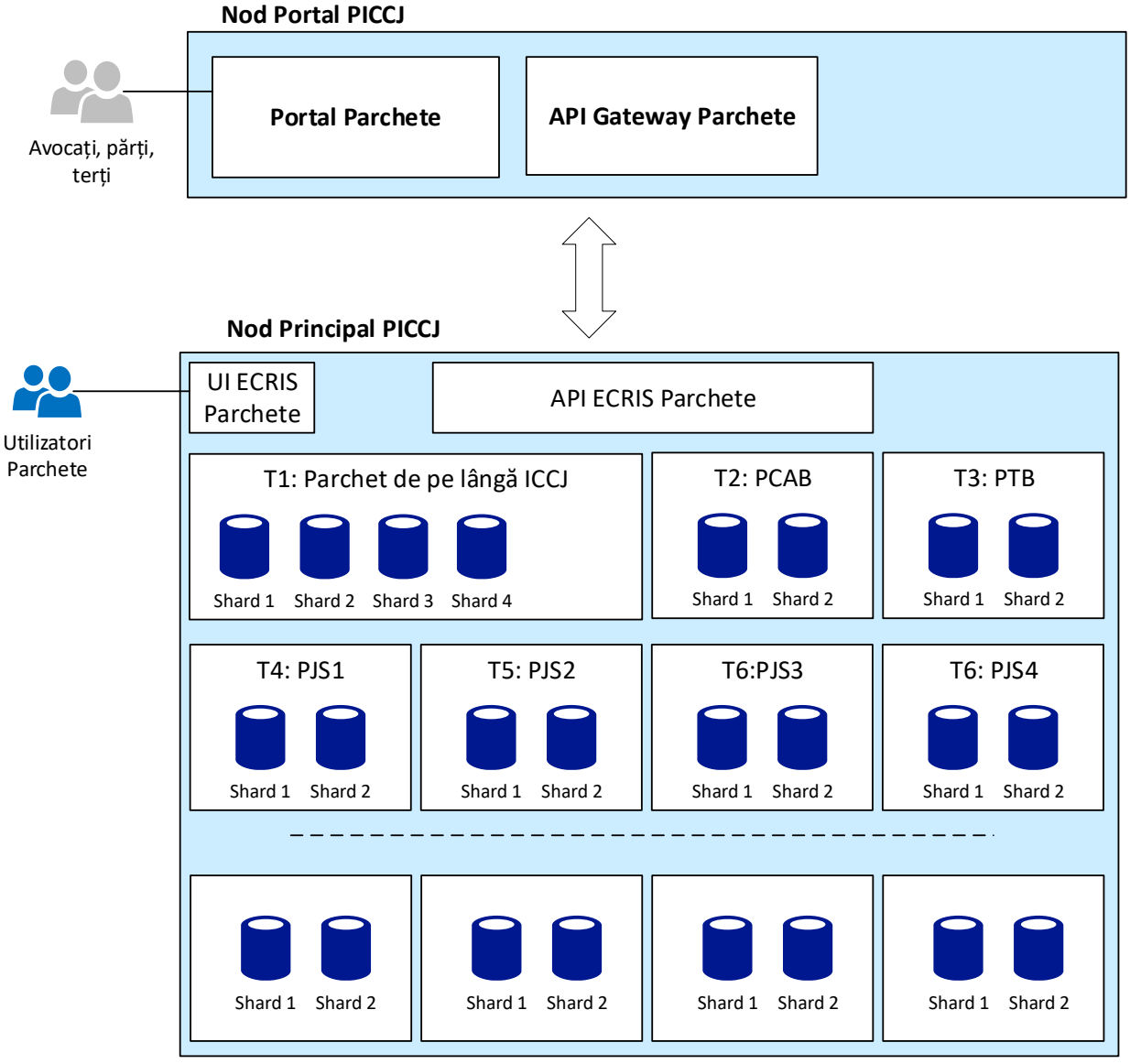


Figure 5 - Instalare PICCJ

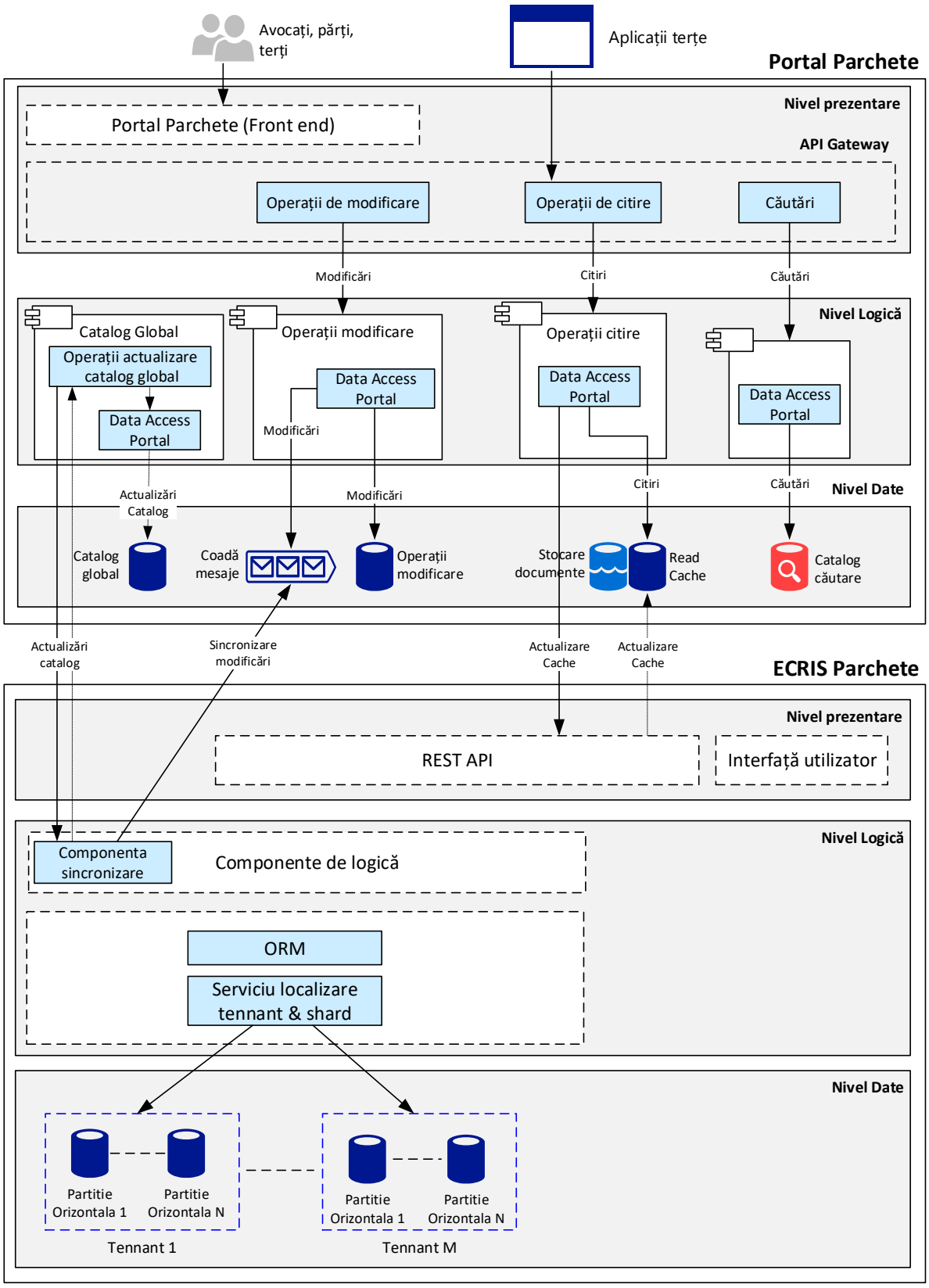


Figure 6 - Integrarea dintre ECRIS Parchete și Portal Parchete

Arhitectura ECRIS Parchete este similară ECRIS Instanțe. De asemenea arhitectura Portalului Parchetelor este similară Portalului Instanțelor. Integrarea dintre ECRIS Parchete și Portalul

Parchetelor va funcționa similar celei dintre ECRIS Instanțe și Portal Instanțe. Pentru a evita redundanțele, conceptele arhitecturale nu vor fi duplicate în cazul Parchetelor.

12.3.2 Informații volumetrice

In tabelul de mai jos sunt sintetizate câteva informații relevante pentru o privire de ansamblu.

Parametru	Valoare
Parametri generali	
Dimensiune stocare / pagina document (MB)	**0.125**
Instanțe	
Utilizatori interni (total angajați din schema de personal)	**12,781**
Nr de request-uri externe / zi. Estimarea se bazează pe traficul actual al portalului Instanțelor înmulțit cu 3, având în vedere ca noul portal va permite și interacțiunea online	**3,000,000**
Medie de dosare noi în fiecare an	**2,117,796**
Cauze soluționate anual	**2,170,715**
PICCJ	
Utilizatori interni (total angajați din schema de personal)	**4,469**
Nr de request-uri externe / zi. Estimare bazată pe traficul actual al portalului Instanțelor împărtit la 3 (având în vedere ca numărul de cauze penale este de aproximativ o treime)	**1,000,000**
Medie de dosare noi în urmărire proprie / an	**29,305**
Medie dosare în urmărire proprie soluționate / an	**22,007**
Medie de dosare noi în supraveghere /an	**615,755**
Medie dosare noi în supraveghere solutionate/an	**534,126**
Medie de lucrări / an	**1,407,106**
Medie lucrări soluționate / an	**1,344,360**
DNA	
Utilizatori interni (total angajați din schema de personal)	**316**
Nr de request-uri externe / zi (portal). 10% din traficul PICCJ	**100,000**
Medie de dosare noi în urmarire proprie / an	**5,143**
Medie dosare în urmarire proprie solutionate / an	**3,226**
Medie de lucrari de solutionat / an	**43,334**
DIICOT	
Utilizatori interni (total angajati din schema de personal)	**940**
Nr de request-uri externe / zi (portal). 20% din traficul PICCJ	**200,000**
Medie de dosare noi în urmarire proprie / an	**9,666**
Medie dosare în urmarire proprie solutionate / an	**8,594**
Medie de lucrari de solutionat / an	**99,007**

12.4 Portal Jurisprudenta

ECRIS CSM

Aplicația va oferi un portal intern de jurisprudență care include documente transmise de ECRIS Instanțe de tip hotărâri, decizii sau încheieri cu textele integrale și rezumate ale acestora, și un portal

public, deschis tuturor utilizatorilor, care conține un subset al documentelor din portalul intern cu texte anonimizate.
Suplimentar, aplicația curentă utilizată în cadrul CSM va comunica cu ECRIS Inspecția Judiciară pentru transmiterea informațiilor despre magistrați, instituții și hotărâri luate în dosarele ce vizează lucrările Inspecției Judiciare și preluarea informațiilor de interes din lucrările de inspecție.

12.4.1 JSP. Portal jurisprudență intern

JSP este un portal de jurisprudență intern a cărui sursă de date va fi ECRIS Instanțe. ECRIS Instanțe va furniza documente de tip hotărâri, decizii, încheieri cu textele integrale și rezumate ale acestora pe baza unor reguli interne (anumite obiecte și materii setate ca fiind relevante etc. , documente aparținând unor dosare fără grad de confidențialitate sau acces restricționat)
Scopul portalului intern este ca judecătorii să nu vină cu soluții total diferite față de cele acordate anterior pentru spețe/decizii similare sau identice. Există cazuri în care o hotărâre pronunțată este atacată, cu posibile rezultate:

- Rămâne soluția acordată
- Se schimbă soluția
- Se trimite spre rejudecare
- Se trimite la altă instanță pe motive de competență.

NOTĂ: Textul rezumat se definește numai în cadrul dosarelor care au o importanță deosebita, așa cum, în prezent, se întâmplă la ICCJ și la nivelul curților de apel.

12.4.2 JEXT. Portal jurisprudență public

JEXT este un portal de jurisprudență public, în care se vor exporta numai anumite documente din portalul intern, cu textele anonimizate.
Vor fi afișate numai documentele care au fost marcate ca fiind publice și au trecut prin procesul de anonimizare manuală a informațiilor

12.5 Portal comunitate

Portalul de comunitate va oferi un spațiu virtual pentru colaborarea dintre profesioniștii din sistemul justiției. Portalul va oferi cel puțin o zonă de articole, zonă de anunțuri și o zonă de colaborare tip forum. Portalul va fi segmentat în funcție de nevoile instituționale, spre exemplu ar putea fi configurat să conțină o zonă comună pentru specialiștii IT din Instanțe, Parchete, Ministerul Justiției și celelalte instituții sau zone separate pentru fiecare instituție.

12.6 Anonimizarea partiala a informatiilor din documente puse la dispozitie prin intermediul portalurilor

Pseudonimizarea este definită în RGPD, articolul 4 punctul 5, ca ”prelucrarea datelor cu caracter personal într-un asemenea mod încât acestea să nu mai poată fi atribuite unei anume persoane vizate fără a se utiliza informații suplimentare, cu condiția ca aceste informații suplimentare să fie stocate separat și să facă obiectul unor măsuri de natură tehnică și organizatorică care să asigure neatribuirea respectivelor date cu caracter personal unei persoane fizice identificate sau identificabile”.

Procesul de anonimizare a datelor desemnează eliminarea tuturor elementelor de identificare dintr-un set de date cu caracter personal, astfel încât persoana vizată să nu mai fie identificabilă. În Avizul 05/2014, Grupul de lucru „Articolul 29" analizează eficacitatea și limitele diferitelor tehnici de anonimizare. Acesta recunoaște valoarea potențială a tehnicilor respective, dar subliniază că anumite tehnici nu funcționează neapărat în toate cazurile. Anonimizarea datelor cu caracter personal se poate efectua static, direct la sursă, sau dinamic în momentul utilizării acestor date.

Cerințele de anonimizare a datelor cu caracter personal din cadru ECRIS au fost identificate pentru modulele portalului de jurisprudență și ale portalului pentru instanțe.

- Cerințele detaliate pentru procesul de anonimizare a datelor cu caracter personal sunt:
  - ✓ Documentele anonimizate automat vor fi verificate manual și de către utilizatori înainte de publicarea acestora.
  - ✓ Utilizatorii vor avea posibilitatea de a compara versiunea inițială cu cea anonimizată prin intermediul unui instrument tehnic care va marca diferențele și zonele de text care sunt susceptibile să conțină date cu caracter personal.
  - ✓ Instrumentul tehnic de anonimizare să aibă o acuratețe bună pentru documentele statice în funcție de conținutul acestora.
  - ✓ Anonimizarea se va baza pe datele structurate despre părți disponibile în primul rând la nivelul dosarului. De multe ori în redactarea unei hotărâri datele se introduc manual, întrucât este mai rapid, așa că pot exista diferențe între datele structurate și textul hotărârii.
- Cerințe tehnice minimale pentru instrumentul tehnic de anonimizare statică:
  - ✓ Asigură identificarea automată a datelor cu caracter personal atât în date structurate (la nivelul dosarului din ECRIS) cât și în date nestructurate (textul hotărârii redactate manual)
  - ✓ Suportă cel puțin următorii algoritmi de căutare a datelor cu caracter personal: expresii regulate (RegEx), valori din dicționar și filtre pe coloane pentru datele structurate;
  - ✓ Suportă cel puțin următorii algoritmi de anonimizare a datelor ce vor fi utilizați selectiv în funcție de cerințele legale:
    - criptare cu păstrarea formatării
    - redactare prin mascarea unui șir de caractere conform unor specificații date
    - filtrare parțială prin omiterea unor caractere
    - generarea unor valori aleatorii.
  - ✓ Permite crearea de reguli personalizate de identificare și anonimizare a datelor cu caracter personal
  - ✓ Asigură integrarea cu baza de date a sistemului ECRIS pentru identificarea automată și anonimizarea datelor;
  - ✓ Anonimizarea trebuie sa fie consistentă în contextul unui document (de exemplu: Partea1 să fie întotdeauna anonimizată Anon1 iar Partea2 să fie întotdeauna anonimizată Anon2 pentru a se asigura același nivel de înțelegere în cadrul documentului.
  - ✓ Asigură identificarea automată și anonimizarea datelor în fișiere nestructurate de tip: text, PDF (text) și Microsoft Office stocate într-un folder local sau în rețea
  - ✓ Asigură integrarea cu soluția de management a logurilor pentru monitorizarea tuturor activităților efectuate.

- Datorită modului în care informațiile sunt publicate prin intermediul portalului ECRIS Instanțe, mascarea datelor trebuie să se realizeze dynamic, în funcție de contextul sesiunii. Daca utilizatorul este autentificat atunci el trebuie să aibă posibilitatea să vizualizeze datele cu caracter personal pentru dosarele unde este parte. Dacă nu este autentificat portalul trebuie să prezinte o versiune anonimizată dinamic a datelor din cadrul portalului.
- Cerințe tehnice minimale pentru instrumentul tehnic de anonimizare dinamică:
    - ✓ Asigură mascarea dinamică a datelor la nivelul aplicației fără a modifica datele în baza de date
    - ✓ Permite identificarea datelor cu caracter personal și aplicarea de politici de anonimizare direct la nivelul aplicației ECRIS fără sa necesite scrierea de cod sau module în aplicație.
    - ✓ Permite crearea de politici de anonimizare, personalizate în funcție de contextul utilizatorului autentificat în aplicație.
    - ✓ Rulează automat procesul de anonimizare, odată ce au fost stabilite politicile, fără să aibă nevoie de intervenție umană
    - ✓ Suportă cel puțin următorii algoritmi de anonimizare a datelor ce vor fi utilizați selectiv în funcție de cerințele legale:
        - criptare cu păstrarea formatării
        - redactare prin mascarea unui șir de caractere conform unor specificații date
        - filtrare parțială prin omiterea unor caractere
        - generarea unor valori aleatorii.
    - ✓ Asigură integrarea cu soluția de management a logurilor pentru monitorizarea tuturor accesărilor de date. Datele de audit trebuie să includă detalii despre modul în care au fost prezentate datele către utilizatori.

13. Statistica Judiciara

Aplicația oferă un modul de raportare comun pentru toate Instanțele de judecată, fiind bazat pe o bază de date comună care include date înregistrate în aplicațiile ECRIS Instanțe. Accesul la rapoarte este limitat printr-un sistem de roluri și permisiuni.

13.1. Statistici Parchete

Aplicația oferă un modul de raportare comun pentru fiecare structură de parchet, fiind bazat pe o bază de date comună care include date înregistrate în fiecare din aplicațiile ECRIS parchete. Accesul la rapoarte este limitat printr-un sistem de roluri și permisiuni. Aplicația va fi instalată distinct pentru PICCJ, DNA și DIICOT.
Pentru raportare se vor folosi baze de date distincte, astfel încât interogările de raportare să nu afecteze performanța aplicațiilor principale. În funcțiile de cerințele de raportare ale aplicației, bazele de raportare pot fi replici OLTP peste care opțional se pot construi baze de date OLAP. Implementarea de baze de date OLAP este recomandată cel puțin pentru aplicațiile de Statistici, ECRIS Instanțe și ECRIS Parchete.

Prin HCSM nr. 1305/2014, secția de judecători a integrat în practica instanțelor, la nivel național, aplicația STATIS, concepută ca un instrument de analiză, de implementare a indicatorilor de eficientă și eficacitate și de măsurare a performanței activității instanțelor.

Pentru evaluarea obiectivă a sistemului judiciar prin intermediul aplicației STATIS au fost identificați următorii indicatori:
I. **Rata de soluționare a dosarelor** (**operativitatea**) calculată exclusiv în raport de dosarele nou intrate - operativitatea se va calcula ca fiind raportul dintre dosarele nou intrate în perioada de referință – respectiv un an de zile – și dosarele finalizate în aceeași perioadă de referință, exprimat procentual;
II. **Stocul de dosare** (mai vechi de un an/1 an și 6 luni) - stocul se va calcula ca fiind suma dosarelor aflate pe rol la finele perioadei de referință și nefinalizate, mai vechi de 1 an pentru curțile de apel și 1 an și 6 luni pentru celelalte instanțe.
III. **Ponderea dosarelor închise într-un an** - reprezintă suma dosarelor soluționate în termen de mai puțin de 1 an de la înregistrare raportată la suma tuturor dosarelor soluționate în perioada de referință la o anumită instanță, exprimată procentual.
IV. **Durata medie de soluționare**, pe materii sau pe obiecte la nivelul fiecărei instanțe și la nivel național (numai pentru stadiul procesual fond și mai puțin pentru curțile de apel) - reprezintă timpul mediu scurs între data înregistrării dosarului („Data dosar" în sistemul ECRIS) și data închiderii documentului. Indicatorul are în vedere valoarea medie a tuturor materiilor vizate (non penal/penal) și este dată de media aritmetică a valorilor acestor materii.
V. **Redactările peste termenul legal** - reprezintă procentul instanței respective de redactare peste termen a dosarelor finalizate cu document de tip final Hotărâre (termenul de redactare este cel incrementat în nomenclatoarele Ecris).
Aplicația poate genera rapoarte statistice corespunzătoare fiecărui indicator de performanță dar și plajelor interne ale acestor indicatori; suplimentar, Statis poate genera și alte rapoarte statistice de interes pentru instanțe și se va adapta permanent cererilor de rapoarte statistice suplimentare venite din teritoriu (spre exemplu, vor putea fi generate informații -inclusiv informații dinamice - structurate pe secții, pe stadii procesuale, pe materii, pe obiecte, pe judecători, privind cauzele nou intrate, soluționate, stocuri de dosare, dosare suspendate, durate medii de soluționare, etc.;
Prin agregarea indicatorilor principali (de eficiență) se poate măsura eficiența activității fiecărei instanțe și se pot întreprinde măsuri pentru a eficientizarea acestei activități fiecare instanță putând fi privită prin prisma particularităților ei și a obiectivelor de management, astfel încât să se poate gândi acele măsuri concrete care să conducă la o mai bună performanță a instanței.
În urma agregării indicatorilor și ca urmare a aplicării unei scale a eficienței și eficacității pentru fiecare indicator în parte, pentru performanta instanțelor se folosesc 4 calificativele: *„foarte eficient", „eficient", „satisfăcător", „ineficient"*. Instanțele cu un grad de eficientă și eficacitate *„satisfăcător"* și *„ineficient"* vor fi supuse verificărilor și analizei de către C.S.M. și de Inspecția Judiciară, acestea vor fi discutate cu instanțele în cauză, care vor fi obligate să implementeze măsurile identificate.

Dependențe: Gestionarea nomenclatoarele comune ECRIS Instante si ECRIS Parchete care se regasesc in cadrul livrabilului L2 - MJ - Specificatii functionale.pdf

14. Probatiune (DNP)

Aplicația gestionează dosarele de probațiune privind evaluarea inculpaților, supravegherea respectării măsurilor și executarea obligațiilor stabilite în sarcina persoanelor supravegheate față de care instanța a dispus: amânarea aplicării pedepsei, suspendarea executării pedepsei sub supraveghere, liberarea condiționată sau executarea pedepsei amenzii prin prestarea unei munci neremunerate în folosul comunității.

14.1 Functionalitati specifice

14.1.1 Elemente de context, cerințe de business și functionalități

Informatiile referitoare la Elemente de context, cerinte de business si functionalitati DNP care trebuie acoperite sunt descrise in cadrul livrabilelor:

- L1.2-Probatiune-Diagrama de context
- L1.2-Probatiune-Diagrame de proces
- L1.2-Probatiune-Elemente de context, cerinte de business si functionalitati cheie ale sistemului
- L1.3-Probatiune-Diagrama entitatilor

14.1.2 Specificații funcționale

Cerințele tehnice și funcționale privind DNP se regasesc in livrabilele:

- L2-Probatiune-Business Object Model
- L2-Probatiune-Model de date detaliat
- L2-Probatiune-Specificatii functionale
- L2-Probatiune-Use case diagram
- L2-Probatiune-Template-uri de documente

14.2 Integarari

Cerinte tehnice si functionale privind acest integrarile DNP se regasesc in livrabilul L2-Probatiune-Specificatii functionale, **Capitolul 3 - Interfete cu alte sisteme**.

15. Inspectia Judiciara

Aplicația gestionează fluxurile de lucru și dosarele din cadrul Inspecției Judiciare. Prima versiune (pilot) a acestei aplicații a fost dezvoltată în cadrul proiectului SIPOCA 55/SMIS 120068. În cadrul aceluiași proiect au fost analizate cerințele viitorului sistem ECRIS și a fost elaborată arhitectura acestuia.
Spre deosebire de celelalte aplicații din sistemul ECRIS, această aplicație nu va fi rescrisă, ci extinsă conform cerințelor de extindere.
Această aplicație va fi extinsă cu noile cerințe și va fi integrată cu celelalte aplicații din sistemul de justiție.

Cerinte tehnice si functionale privind Inspectia Judiciara se regasesc in livrabilul/livrabilele…

- L2-IJ-Specificatii functionale faza II

16. Administrare

Pentru a reduce riscul ca administratorii sistemului ECRIS să expună din greșeală conturile privilegiate pe computerele cu risc de securitate mare este necesară implementarea unui sistem centralizat de management al accesului privilegiat.
Soluția de administrare a accesului privilegiat (PAM – Privileged Access Management) asigură monitorizarea și controlul accesului utilizatorilor cu drepturi privilegiate la echipamentele de tip server din cadrul ECRIS permițând concomitent monitorizarea activităților acestora.
Soluția administrează accesul utilizatorilor la sisteme, creează și aplică o politică de acces pentru utilizatorii interni și externi și suportă crearea unor reguli de autorizare pentru acordarea sau interzicerea accesului la resurse.

Cerințe minime:

- Accesul la serverele din cadrul sistemului ECRIS prin intermediul credențialelor privilegiate se va putea face prin intermediul stațiilor de lucru de tip bastion;
- Nu este permisă utilizarea credențialelor privilegiate direct de pe stația de lucru a administratorului.
- Utilizatorul normal al administratorului (contul neprivilegiat) ce este folosit de acesta pentru a se autentifica pe stația de lucru si pentru navigarea pe Internet sau utilizarea Email-ului nu va avea asignate drepturi privilegiate pe serverele din cadrul ECRIS;
- Asignarea drepturilor privilegiate se va face automat de către soluția de administrare a credențialelor privilegiate prin intermediul politicilor definite în prealabil;
- Drepturile privilegiate vor fi asignate doar atâta timp cat e nevoie;
- Utilizatorii vor primim doar drepturile privilegiate necesare pentru efectuarea activității dorite;
- Administratorul poate solicita alocarea unor drepturilor privilegiate prin intermediul unor fluxuri de aprobare;
- Fluxurile de aprobare trebuie să poată fi personalizate astfel încât să asigure o utilizare ușoară a acestora;
- Utilizarea drepturilor privilegiate este auditată iar evenimentele sunt centralizate prin intermediul soluției de management al jurnalelor de audit.

Volumetrie

ECRIS Instanțe

- Soluția trebuie să asigure administrarea centralizată a conturilor privilegiate din cadrul ECRIS Instanțe, inclusiv pentru infrastructura de suport și componenta BCDR

ECRIS Parchete

- Soluția trebuie să asigure administrarea centralizată a conturilor privilegiate din cadrul ECRIS Parchete, inclusiv pentru infrastructura de suport și componenta BCDR.

Se va furniza o soluție de sine stătătoare pentru fiecare entitate care utilizează ECRIS Parchete (PICCJ, DNA și DIICOT)

16.1 Atribuire/Definire Roluri Utilizator si drepturi de acces

Securizarea accesului la modulele aplicației (autorizare)

Sistemul trebuie să pună la dispoziția utilizatorilor accesul la diverse module ale aplicației pe baza drepturilor de acces descrise in profilul utilizatorului.

Administratorii vor avea posibilitatea de a defini roluri multiple de securitate, la nivel de ecran, la nivel de componentă logică (ex: dosar / lucrare) și la nivel de operație efectuată (citire, scriere, modificare, ștergere, printare).

Utilizatorii vor putea fi asociați la rolurile definite la nivelul fiecărei componente a sistemului și vor primi drepturi în aplicație în funcție de acestea.

Aplicația trebuie sa permită ca ulterior, utilizatorii sa primească drepturi suplimentare sau sa li se restrângă drepturile, in funcție de nevoile specifice.

16.2 Audit

16.2.1 Jurnalizare erori aplicație

Sistemul trebuie să ofere capabilități de jurnalizare a erorilor de aplicație, în funcție de severitatea acestora. Nivelul la care se face jurnalizarea va fi configurabil și se va putea face la unul din următoarele nivele de severitate: fatal, erori, alerte, debug, informativ, descriptiv.

Erorile vor înregistra, pe lângă mesajul specific de eroare și modulul (componenta software) care a generat eroarea, pe ce sistem a fost generată, ce utilizator era logat, data și ora aferente.
Sistemul va permite administratorilor consultarea informațiilor disponibile referitoarea la erorile generate de aplicație, cu posibilități de filtrare, căutare, etc.

16.2.2 Detaliere erori de aplicație

Sistemul trebuie să ofere capabilități de detaliere a erorilor de aplicație cu mesaje de eroare descriptive care sa conțină minim: stare endpoint serviciu, proces apelant, timp de răspuns, momentul înregistrării etc.
Înregistrările de jurnalizare trebuie să conțină minimum detalii despre

- ID-ul Sesiunii la care se referă mesajul
- ID-ul modulului/aplicației care a generat mesajul și numele modulului/aplicației,
- ID-ul utilizatorului logat in momentul generării mesajului și numele utilizatorului,
- ID-ul mesajului generat și mesajul generat.
- Severitatea mesajului
- Data și ora la care a fost generat mesajul in format YYYY-MM-DD HH-MM-SS

16.3 Administrare Nomenclatoare

ECRIS Admin
Aplicația ECRIS Admin cumulează funcționalități de administrare a sistemelor ECRIS, spre exemplu administrarea nomenclatoarelor globale.

16.4 Administrare si Generare Rapoarte (operationale sau statistice)

Cerintele tehnice se vor detalia in etapa de Analiza Detaliata.

16.5 Administarea repartitiei aleatoare a dosarelor

Cerintele tehnice se vor detalia in etapa de Analiza Detaliata.

16.6 Monitorizare și jurnalizare

16.5.1.1 Gestionare centralizată a elementelor monitorizate

Sistemul trebuie să pună la dispoziție administratorilor mecanisme de vizualizare a elementelor monitorizate, a stării lor (healthy, degraded, etc) într-un format grafic, ușor de urmărit, astfel încât să poată fi identificate elementele care sunt cu probleme.
Sistemul va pune la dispoziția utilizatorilor mecanisme de codificare prin culori a stărilor diferitelor elemente monitorizate, astfel încât să fie ușor identificabile cele cu probleme.

16.5.1.2 Monitorizare aplicație

Sistemul trebuie să ofere instrumente de monitorizare pentru aplicațiile dezvoltate, atât la nivel de server de aplicație (web server) dar și la nivel de procese specifice aplicației.
Sistemul de monitorizare va permite monitorizarea parametrilor specifici aplicației, care includ:
- Monitorizarea punctelor expuse via HTTPS (Endpoint monitoring)
- Monitorizarea timpilor de încărcare pentru paginile web
- Monitorizarea certificatelor SSL/TLS pentru expirare
- Monitorizarea serverului de aplicație (disponibilitate, erori)

16.5.1.3 Monitorizare baze de date

Sistemul trebuie să ofere instrumente de monitorizare pentru parametrii de la nivelul bazei de date și includ:
- Capacitatea de stocare a bazei de date
- Volumele de tranzacții procesate concurent
- Performanța interogărilor pe baza de date
- Conflictele de tip deadlock apărute

16.5.1.4 Monitorizare utilizatori

Sistemul trebuie să ofere instrumente de monitorizare a activităților utilizatorilor, inspectând informațiile jurnalizate despre activitatea utilizatorului și alte informații disponibile și identificând șabloane referitoare la activitate suspectă (ex: încercarea de a accesa sistemul din afara rețelei, de pe mai multe stații în paralel).
Astfel de activități suspecte vor fi notificate administratorilor pentru a putea identifica eventualele vulnerabilități în interiorul organizației (ex: utilizatori care urmăresc preluarea sau modificarea neautorizată de date). Canalele de comunicare vor fi multiple (in aplicate si e-mail), nivelul si canalul de comunicare a alertelor vor fi configurabile.

16.5.1.5 Mecanisme de alertare a administratorilor

Sistemul trebuie să ofere posibilitatea administratorilor de a defini alerte în cazul în care se îndeplinesc anumite criterii (ex: încărcarea discului depășește 90% și poate deveni o problemă).
Administratorii vor avea posibilitatea de a seta mai multe astfel de tipuri de notificări, în funcție de necesități.
Notificările vor fi transmise prin email sau vor fi disponibile în interfața de administrare a uneltei de monitorizare pentru consultare.

16.5.2 Securizarea accesului aplicației la componentele sistemului de operare

Sistemul trebuie să pună la dispoziția administratorilor mecanisme prin care aplicația să poată fi folosită utilizând un set minimal de permisiuni de acces la nivelul sistemului de operare și al infrastructurii de aplicație.
Utilizarea aplicației va trebui să fie posibilă și fără conturi cu drepturi administrative asupra sistemului de operare (ex: local administrator, domain administrator, etc).

17. Sisteme suport

17.1 ECRIS Admin

Aplicația ECRIS Admin cumulează funcționalități de administrare a sistemelor ECRIS, spre exemplu administrarea nomenclatoarelor globale.

17.2 Portal Comunitate

Portalul de comunitate va oferi un spațiu virtual pentru colaborarea dintre profesioniștii din sistemul judiciar. Portalul va oferi cel puțin o zonă de articole, zonă de anunțuri și o zonă de colaborare tip forum. Portalul va fi segmentat în funcție de nevoile instituționale, spre exemplu ar putea fi configurat să conțină o zonă comună pentru specialiștii IT din Instanțe, Parchete, Ministerul Justiției și celelalte instituții sau zone separate pentru fiecare instituție.

17.3 Sistem suport și KB

Sistemul de suport va oferi funcționalitățile tipice unui sistem de suport, printre care: management incidente, multi-agent, suport comunicare multi-canal (email, telefon, sms etc), evidenta SLA, statistici suport, șamd. Sistemul de suport va fi folosit în comun de instituțiile sistemului de justiție, dar fiecare instituție va avea o secțiune separată precum și personal dedicat alocat sistemului de suport.
O funcționalitate importanta a sistemului de suport este aceea de Knowledge Base. în zona de knowledge base (baza de date de cunoștințe) vor fi acumulate toate materialele de suport și documentele relevante pentru suportul sistemului. Spre exemplu, pentru problemele frecvente pentru care utilizatorii solicita suport, personalul de suport va dezvolta în timp materiale reutilizabile (ex: procedura de înregistrare a unui cont nou), astfel încât efortul personalului de suport sa fie eficientizat. Zona de knowledge base va fi disponibila direct utilizatorilor în cadrul portalului de comunitate (self service).

17.4 Infrastructura Medii suport (DevOps)

Acest sistem va conține ansamblul aplicațiilor și instrumentelor necesare pentru a susține ciclul de viață al aplicațiilor software: mediile de dezvoltare, testare și acceptanță, instrumentele de dezvoltare, sistemul de control al codului sursa (source control), sistemele de testare automata, sistemele de continuous delivery șamd.

Sistem de management al infrastructurii
Sistemul va asigura monitorizarea și managementul centralizat al infrastructurii cuprinzând echipamentele hardware, tehnologia de virtualizare, sistemele software instalate (COTS), comunicațiile și aplicațiile instalate.

18. Tranzitie

18.1 Migrare date

Pentru instalarea în producție a noilor versiuni ale aplicațiilor ECRIS este necesară migrarea datelor din bazele de date actuale în noile baze de date. În acest sens furnizorul va asigura design-ul, dezvoltarea și testare unor instrumente automate care vor fi folosite în faza de instalare pentru migrarea datelor în mediul de producție. Instrumentele de migrare și în special migrarea datelor vor face obiectul procesului final de acceptanță.

18.1.1 Strategie Migrare

Obiectivul principal al migrării este transferarea integrală a datelor folosite de fiecare instituție beneficiară, respectiv toate instanțele de judecată, PICCJ, DNA, DIICOT și Inspecția Judiciară, din bazele de date anterioare în noile baze de date, în momentul în care noile aplicații sunt lansate în producție.
În acest sens este necesară dezvoltarea a patru instrumente/proiecte distincte:

- Instrument pentru migrarea datelor folosite de instanțe;
- Instrument pentru migrarea datelor folosite de parchete PICCJ;
- Instrument pentru migrarea datelor folosite de parchete DIICOT;
- Instrument pentru migrarea datelor folosite de DNA;

Pentru fiecare astfel de proiect furnizorul va realiza cel puțin următoarele activități:

- Analiza cantitativă si calitativă a datelor
- Design detaliat
- Dezvoltarea instrumentelor de migrare
- Documentație de operare și coexistență
- Migrarea datelor și testare

18.1.1.1 Analiza cantitativă și calitativă a datelor

Furnizorul va realiza o analiză calitativă și cantitativă a datelor existente care va urmări să determine eventualele probleme de calitate a datelor (integritate relațională, date duplicate, date invalide etc.). Bazele de date ce fac obiectul migrării au fost folosite de instituții beneficiare pentru o perioadă suficient de lungă de timp, astfel încât, deși nu poate fi garantat, este probabil ca datele să fie în general consistente. Cu toate acestea o analiză prealabilă a datelor existente este necesară pentru a identifica și rezolva eventualele probleme ce pot genera riscuri pentru migrare.
Activitatea de analiză se va concretiza cu un raport de analiză care va identifica potențialele probleme și măsurile propuse de soluționare. Toate problemele de consistență a datelor pentru care există o soluție de rezolvare automată, vor fi rezolvate de furnizor prin implementarea instrumentelor de migrare.

18.1.1.2 Design detaliat

Furnizorul va realiza un document de design detaliat al migrării care va cuprinde cel puțin următoarele elemente:

- Un model de migrare (mapare) între noua bază de date și bazele de date existente, astfel pentru fiecare tabelă și câmp din noile baze de date se va defini sursa de date, respectiv tabela și câmpul din bazele de date existente și viceversa;
- Modelul de migrare trebuie să fie complet, respectiv:
  - ✓ Pentru toate entitățile din bazele de date existente trebuie să existe o entitate destinație în noile baze de date. În caz contrar trebuie validat că entitatea respectivă nu trebuie să fie migrată, respectiv entitatea respectivă nu va mai fi folosită în noua aplicație;
  - ✓ Pentru toate atributele entităților existente trebuie să existe un atribut destinație în noile baze de date. În caz contrar trebuie validat că atributul repectiv nu este necesar pentru migrare, respectiv nu va mai fi folosit în noua aplicație;
  - ✓ Pentru toate entitățile existente în noile baze de date există o entitate asociată în bazele existente, cu excepția entităților nou apărute în noua versiune;

  - ✓ Pentru toate atributele entităților existente în noile baze de date există un atribut asociat în bazele existente, cu excepția atributelor noi pentru care aplicațiile trebuie să asigure un tratament adecvat (respectiv tratarea cazurilor de NULL);
  - ✓ Migrarea datelor de referință (nomenclatoare) va fi consistentă
- Secvența activităților de migrare, care va indica ordinea migrării diferitelor obiecte din bazele de date vechi;
- Identificarea regulilor de migrare aplicabile și a parametrilor de configurare aferenți pentru cazurile de conflicte între datele sursă și datele destinație în cazul migrărilor repetate (reluarea migrării folosind aceleași baze de date);
- Mecanismele de auditare a migrării;
- Mecanismele de logging tehnic;
- Mecanismele de testare post migrare;
- Asigurarea caracteristicii tehnice de idempotență a instrumentelor de migrare;
- etc

Pentru versiunile noi ale aplicațiilor ECRIS Parchete, ECRIS Instanțe, ECRIS DNP, în cadrul proiectului SIPOCA55 au fost realizate modele de date conceptuale. Acestea se regăsesc în cadrul livrabilului 2. Specificatii software. Aceste modele pot ghida procesul de proiectare detaliată a noilor baze de date și conțin o parte din mapările cu bazele de date existente.

18.1.1.3 Dezvoltarea instrumentelor de migrare

Pe baza documentului de design detaliat furnizorul va dezvolta instrumentele de migrare, care trebuie să respecte cel puțin următoare caracteristici tehnice:
Idempotență – instrumentele de migrare trebuie să fie idempotente, astfel încât să poată fi executate de mai multe ori folosind aceleași baze de date sursă și destinație. Astfel instrumentele de migrare trebuie să funcționeze diferențial, respectiv să determine diferențele dintre sursă și destinație și să aplice un set de reguli de migrare configurabile care să permită diverse scenarii de migrare (ex: suprascrierea unor date deja migrate indiferent de starea acestora, ignorarea unor date dacă sunt diferite între sursă și destinație etc.). Această caracteristică va fi esențială la migrarea go-live a datelor, în special în cazul instanțelor (spre exemplu pentru a relua o eventuală migrare eșuată).
Migrare parțială / discretă – instrumentele de migrare trebuie să permită migrarea unei submulțimi de entități din bazele de date sursă. Această caracteristică va fi utilă pentru a rezolva eventuale erori de migrare ulterior intrării în producție a noilor aplicații, dar posibil și pentru a simplifica procedurile de coexistență în cazul instanțelor. Posibilitatea de a migra un singur dosar va fi folosită pentru a migra dosare transferate (descrisă în capitolul 3.5.2 – Proceduri de coexistență).
Audit detaliat - instrumentele de migrare trebuie să auditeze integral procesul de migrare. Auditul trebuie să cuprindă atât informații despre entitățile migrate cu succes cât și despre avertismentele sau erorile de migrare apărute și informații detaliate despre fiecare eroare sau avertisment.
Log tehnic detaliat - erorile tehnice de migrare trebuie de asemenea salvate cu toate detaliile necesare analizării ulterioare.
Raportare migrare – la finalul unei migrări instrumentele de migrare vor genera în mod automat un raport de migrare care va cuprinde un sumar al migrării. Acest raport trebuie să cuprindă chei de control cantitative care să permită o evaluare rapidă a rezultatului migrării. Informații minime care trebuie să fie conținute de raport:

- nr total de entități în bazele sursă ce au fost în scopul migrării vs nr entități migrate
- pentru fiecare tip de entitate: nr de entități sursă, nr entități destinație migrate cu succes, nr entități migrate cu avertisment, nr de entități eșuate
- nr de erori din fiecare categorie (cast nereusit etc)

- nr de avertismente din fiecare categorie (e.g. trunchiere texte, cast cu pierderi de precizie etc)

Performanță - performanța instrumentelor de migrare este critică în special în cazul instrumentelor destinate instanțelor. În mod ideal migrarea datelor unei instanțe (inclusiv Tribunalul București) nu ar trebui să dureze mai mult de patru ore. În cel mai defavorabil caz migrarea datelor nu va depăși 24 ore. Performanța instrumentelor de migrare va fi esențială în faza de migrare pentru a asigura o migrare rapidă și eficientă.

Anonimizare surse – având în vedere sensibilitatea informațiilor din bazele de date sursă, instrumentele de migrare vor fi folosite de specialiștii IT ai instituțiilor beneficiare. Pentru a putea dezvolta și testa instrumentele de migrare furnizorul va trebui să dezvolte și instrumente de anonimizare a bazelor de date sursă. Aceste instrumente vor fi folosite de instituțiile beneficiare pentru a genera baze de date de test care vor conține un subset de date anonimizate.

IMPORTANT: pentru testarea și stabilizarea instrumentelor de migrare dedicate instanțelor se vor folosi în mod obligatoriu bazele de date ale grupului de instanțe București, respectiv Înalta Curte de Casație și Justiție, Curtea de Apel București, Tribunalul București, Judecătoriile Sectorului 1-6. Acest grup de instanțe dispune de cel mai mare volum de date și cea mai mare complexitatea a informației, astfel testarea folosind bazele de date ale acestor instanțe va reduce considerabil riscurile pentru migrările celorlalte instanțe.

Pentru testarea și stabilizarea instrumentelor de migrare dedicate parchetelor se vor folosi în mod obligatoriu bazele de date ale grupului de parchete București, respectiv parchetul de pe lângă Înalta Curte de Casație și Justiție, parchetul de pe Curtea de Apel București, parchetul de pe Tribunalul București, parchetele de pe Judecătoriile Sectorului 1-6, DIICOT și DNA.

18.1.1.4 Documentație de operare

Furnizorul va realiza o documentație de operare detaliată a instrumentelor de migrare care va cuprinde cel puțin următoarele detalii:

- Exemple de utilizare
- Descrierea detaliată parametrilor de configurare
- Documentația erorilor
- Explicații privind conținutul raportului de migrare
- etc.

18.1.1.5 Migrarea datelor și testare

Planul propus pentru migrare este detaliat în metodologia de proiect. Migrările tuturor bazelor de date trebuie să finalizate cu succes cel târziu cu trei luni înainte de finalizarea proiectului ECRIS.

8.1.2 Cerinte de Securitate a Migrarii Datelorl

Migrările de date sunt în general deosebit de susceptibile la întreruperi temporare ale securității. Cu cât migrarea este mai complexă, cu atât există mai multe oportunități pentru erorile de securitate. Abordarea acestor posibile probleme de securitate se face cel mai bine mai întâi prin conștientizarea problemei și apoi prin proiectarea meticuloasă a migrării acestora având aspectele de securitate în minte. Întotdeauna planificarea, proiectarea și testarea metodei de migrare cu o analiză riguroasă pe securitate este cheia într-o migrare de succes.

Principalele domenii de risc la migrarea datelor sunt:

- Disponibilitatea – Asigurarea unei ferestre de mentenanță care să permită finalizarea tuturor pașilor definiți în procedura de migrare, inclusiv backup-ul complet inițial și eventual timpul necesar de întoarcere la starea inițială daca procesul eșuează. Pe parcursul acestei ferestre de mentenanță datele migrate nu trebuie se fie modificate.
- Confidențialitatea – Asigurarea unui nivel de confidențialitate cel puțin egal cu cel din sistemul ECRIS sursă. Alinierea modelelor de securitate și control al accesului (vezi detaliile de mai jos)
- Integritatea – Asigurarea migrării tuturor datelor fără modificarea acestora. Se recomandă implementarea unor cheii de control pe seturile de date, crearea de hash-uri pentru fișierele temporare (imediat după export și imediat înainte de import), evaluarea aleatorie a unor seturi de date înainte și după migrare
- Adoptarea – asigurarea migrării utilizatorilor și aplicației vechi de pe vechiul sistem ECRIS pe noul sistem ECRIS după finalizarea procesului de migrare. Blocarea la scriere a bazei de date vechi și decomisionarea acesteia în siguranță conform planului de migrare.

Considerațiile de securitate pentru migrările de date efectuate în vederea trecerii la noul ECRIS sunt:

- Evaluarea modelului actual de securitate și a modului în care acesta este utilizat.
- Identificarea diferențelor și planificarea actualizării acestuia astfel încât să se potrivească cu noul model de securitate (îmbunătățit). Aspectele cele mai importante de urmărit în procesul de actualizare a modelului de securitate sunt:
  - ✓ Îmbunătățirea controlul accesului la date pe perioada migrări. Creșterea drepturilor de acces la date trebuie să fie temporară, justificată și auditată. Dacă este necesară utilizarea unui utilizator cu drepturi extinse, pe perioada migrării, în vederea garantării accesului la toate datele ce vor fi migrate se vor implementa măsuri compensatorii de protecție și monitorizare a accesului.
  - ✓ Implicarea echipei de securitate în stabilirea și revizuirea planului de migrare.
- Asigurarea nivelului corespunzător de securitate a datelor pe perioada migrării prin implementarea de controale. Aceste controale trebuie să asigure cel puțin:
  - ✓ Criptarea datelor pe perioada migrării dacă se utilizează zone tampon de stocare în cadrul procesului
  - ✓ Identificarea și implementarea de cheii de control pentru asigurarea integrității datelor în procesul de migrare.
  - ✓ Asigurarea unei procesări limitate la scopul migrării prin eliminarea oricăror accesări inutile la date.
  - ✓ Auditarea tuturor activităților efectuate pe parcursul procesului de migrare. La finalul migrării se va genera un raport de audit ce va include detalii complete despre utilizatorii care au accesat datele și nivelul de acces al acestora (citire / scriere).
  - ✓ Ștergerea permanentă a oricăror zone temporare de stocare a datelor folosite pe parcursul migrării.

18.1.3 Acceptanță Migrare

Acceptanța migrărilor se va realiza la finalul proiectului, ca parte din procesul general de acceptanță.
Criteriile de acceptanță a activității de migrarea vor urmări migrarea integrală a datelor din toate bazele de date avute în scop în noile baze de date ECRIS, respectiv:

- Toate bazele de date ECRIS CDMS utilizate de către instanțe

- Toate bazele de date SAE utilizate de către instanțe
- Toate bazele de date ECRIS Prosecutors utilizată de PICCJ și instituțile subordonate.
- Toate bazele de date SAE utilzată de PICCJ și instituțile subordonate.
- Baza de date ECRIS Prosecutors utilizată de DIICOT
- Baza date a aplicațiilor utilizate de către DNA
- Baza de date SAE utilzată de DNA

18.2 Instruire

Aceasta componenta nu este in scopul actualei etape de Consultare de piata.

18.2.1 Strategie Instruire

18.2.2 Instruire Tehnica

18.2.3 Instruire Functionala

18.3 Roll-out

Aceasta componenta nu este in scopul actualei etape de Consultare de piata.

19. Garantie si support post roll-out

19.1 Suport

19.1.1 Bune practici în dezvoltarea aplicației

Furnizorul trebuie să asigure dezvoltarea codului folosind o metodologie de dezvoltare cunoscută și acceptată de industrie, pusă la dispoziția beneficiarului.
În cadrul dezvoltării aplicației se vor lua în considerare cel puțin:

- ✓ Denumire unitară fișiere aferente aplicației
- ✓ Denumire unitară și descriptivă a variabilelor folosite
- ✓ Organizarea concisă a codului și simplitatea în înțelegere
- ✓ Eficiența algoritmilor utilizați
- ✓ Fiabilitate și ușurință în menținere / dezvoltare ulterioară
- ✓ Mecanisme de testare unitară a codului (unit test)

19.1.2 Versionarea sistemului

Sistemul trebuie să pună la dispoziția administratorilor și utilizatorilor mecanisme de versionare a componentelor acestuia (ex: aplicație web, bază de date, module DLL, etc).
Versionarea va respecta principiile versionării semantice (MAJOR.MINOR.PATCH) disponibile pe https://semver.org/ pentru fiecare componentă.

- MAJOR – o versiune care include modificări incompatibile cu versiunea anterioară
- MINOR – o versiune care aduce funcționalități noi, dar este compatibilă cu versiunea anterioară
- PATCH – o versiune creată atunci când se rezolvă un defect software

Un registru complet ar fiecărei versiuni, cu modificările aferente va fi disponibil pentru fiecare componentă și va putea fi consultat de administratorii desemnați ai sistemului.

19.1.3 Strategie publicare actualizări

Software-ul dezvoltat în cadrul implementării va avea o strategie de publicare a actualizărilor software, în funcție de defectele identificate, folosind mecanisme de tipul CI/CD (Continuous Integration / Continuous Delivery).
Strategia de actualizare va include informații cel puțin despre:
- Politicile de publicare pentru versiuni majore
- Politicile de publicare pentru versiuni minore
- Politicile de publicare pentru patch / hotfix
- Ferestre de mentenanță (în cazul în care sunt necesare)

19.1.4 Testabil

Sistemul trebuie să fie unul ușor testabil, în special în mod automat. În acest sens pe parcursul dezvoltării, furnizorul va dezvolta teste automate care vor acoperi cel puțin 80% din funcționalitate și cu prioritate funcționalitățile frecvent utilizate.

19.1.5 Gestionarea actualizărilor

Gestionarea actualizărilor (Patch Management) este procesul de identificare, achiziționare, instalare și verificare a patch-urilor pentru aplicații și sisteme de operare. Patch-urile corectează probleme de securitate și funcționalitate în software și firmware. Din punct de vedere al securității, patch-urile sunt cel mai adesea de interes, deoarece acestea atenuează vulnerabilitățile defectelor software; aplicarea de patch-uri pentru a elimina aceste vulnerabilități reduce semnificativ oportunitățile de exploatare.
Upgrade-urile pot remedia, de asemenea, problemele de securitate și funcționalitate în versiunile anterioare de software și firmware, menținându-le astfel și la o versiune acceptată și actuală.
Cerințele minime pentru implementarea unui proces de gestionare a patch-urilor și actualizărilor software in cadrul ECRIS sunt:
• Soluția propusă trebuie să asigure gestiunea integrată a patch-urilor și actualizărilor software atât pentru sistemele de operare cat și pentru aplicațiile instalate.
•Trebuie să includă funcționalități complete de inventariere hardware, software și utilizare a licențelor pentru soluțiile incluse in ECRIS
• Trebuie să includă un set de instrumente și resurse care să permită raportarea avansată pentru inventarierea software, hardware și gestiunea patch-urilor.
• Permite definirea de fluxuri automate sau manuale de aplicare a patch-urilor
• Trebuie să permită integrarea cu soluția de management al jurnalelor de audit astfel încât să asigure o imagine integrată asupra managementului vulnerabilităților de la detecție până la remediere prin aplicarea patch-ului.

ECRIS Instanțe
• Soluția trebuie să asigure administrarea centralizată a patch-urilor tuturor componentelor din ECRIS Instanțe, inclusiv infrastructura de suport și componenta BCDR
ECRIS Parchete
• Soluția trebuie să asigure administrarea centralizată a patch-urilor tuturor componentelor din ECRIS Parchete, inclusiv infrastructura de suport și componenta BCDR.
• Se va furniza o soluție de sine stătătoare pentru fiecare entitate care utilizează ECRIS Parchete (PICCJ, DNA și DIICOT)

19.1.6 Validarea de securitate a actualizărilor software înainte de publicare

Sistemul trebuie să permită scanarea automată de vulnerabilități cunoscute și de bune practici de programare a versiunilor propuse spre actualizare, înainte ca acestea să fie publicate către utilizatori.

Sistemul va permite blocarea publicării versiunii în cazul în care sunt identificate defecțiuni de programare sau vulnerabilități de natură să afecteze buna funcționare a sistemului.

19.1.7 Semnare electronică a actualizărilor sistemului

Sistemul trebuie să permită utilizarea mecanisme de verificare a integrității codului care va fi folosit pentru actualizarea sistemului, prin semnarea digitală a binarelor publicate folosind certificate calificate, emise în acest scop.
Sistemul va oferi posibilitatea activarii unor mecanisme care sa nu permită instalarea de actualizări care nu au semnătura electronică validă, astfel încât să fie protejat de modificări neautorizate.

19.1.8 Documentație AS-BUILT

Furnizorul trebuie să pună la dispoziția beneficiarului o documentație actualizată care să reflecte modul în care a fost construit sistemul, luând în calcul toate modificările survenite în cadrul implementării (din varii motive).

19.1.9 Documentație de utilizare

Furnizorul trebuie să pună la dispoziția beneficiarului documentație de utilizare (manuale și ghiduri specifice de utilizare) pentru fiecare componentă aplicativă din cadrul sistemului (componente software dezvoltate pentru sistemul informatic). Documentația de utilizare va identifica fiecare rol și va identifica instrumentele și funcționalitățile disponibile și aplicabile pentru fiecare rol în parte.
Manualele vor fi disponibile în format electronic și vor forma baza cursurilor de utilizare pentru fiecare rol în parte.

19.1.10 Documentație de administrare

Furnizorul trebuie să pună la dispoziția beneficiarului documentație de administrare (manuale și ghiduri specifice de administrare), necesare unei bune administrări a sistemului.
Fiecare componentă care face parte din mecanismele de administrare va fi descrisă și explicată, astfel încât sistemul să fie înțeles de către administratorii desemnați din partea beneficiarului.
Manualele vor fi disponibile în format electronic și vor forma baza cursurilor de utilizare pentru fiecare rol în parte.

9.1.11 Documentarea codului sursă

Furnizorul trebuie să pună la dispoziția beneficiarului documentație aferentă codului sursă, pentru fiecare modul și componentă a aplicațiilor dezvoltate. Documentația va fi în limbile română sau engleză, în mod unitar pentru tot codul și va fi disponibilă pentru fiecare metodă dezvoltată.

9.1.12 Proprietatea intelectuală a codului aparține beneficiarului

Proprietatea intelectuală asupra componentelor software ECRIS dezvoltate în cadrul proiectului aparține beneficiarului, iar codul sursă al aplicațiilor nu va fi făcut public. Furnizorul va pune la dispoziția beneficiarului, la finalizarea implementării, codul sursă împreună cu toate componentele necesare pentru construirea fiecărui modul de aplicație.
În cazul folosirii unor componente terțe (third-party) furnizorul trebuie să se asigure că licența componentei este compatibilă cu sistemul ECRIS. În cazul folosirii de componente open source se vor

folosi doar componente cu licențiere tip BSD sau echivalent (BSD, MIT). Nu se vor folosi licențe tip GNU GPL, inclusiv LGPL sau orice altă licență care obligă la publicarea codului sursă derivat în domeniul public. În cazul componentelor comerciale se vor folosi doar licențe tip "Royalty free", de asemenea Furnizorul va asigura licențierea componentelor comerciale inclusiv pentru personalul beneficiarului, astfel pentru fiecare componenta comercială se vor asigura 10 licente de dezvoltare. Nu se vor utiliza componente comerciale care presupun licențe cu cost variabil in funcție de numărul de proiecte, site-uri, volum de utilizare sau orice altă variabilă, decât cu acordul formal al beneficiarului.
De asemenea, furnizorul va pune la dispoziția beneficiarului manuale care descriu modalitatea prin care fiecare componentă software poate fi construită din surse, inclusiv cu versiuni de librării folosite și versiuni minime de medii de dezvoltare utilizate.

19.2 Componente COTS

19.2.1 Planificarea actualizărilor componentelor COTS

Pentru componentele COTS, tipul de conținut al actualizărilor si o analiza de impact (actualizări de securitate, actualizări de funcționalitate, etc) va fi prezentat în avans beneficiarului. Data și necesitatea actualizărilor se vor stabili în funcție de fiecare pachet propus pentru actualizare, dar și de politicile de IT ale MJ şi ale celorlalte instituții partenere din sistemul judiciar.

19.2.2 Matricea de compatibilitate a componentelor COTS

La darea in folosință a sistemului, beneficiarul va primi o matrice de compatibilitate a versiunilor între diversele componente comerciale folosite (ex: Sistem de operare, Motor de baze de date, browser etc) care va include și perioada pentru care producătorul oferă suport pentru versiunea respectivă de produs software.

19.3 Garantie si Suport

19.3.1 Garanție de 2 ani de la darea în exploatare

Furnizorul trebuie să includă în oferta tehnică servicii de garanție ale întregului sistem pe o perioadă de 24 luni de la punerea în funcțiune a acestuia. În toată această perioadă, furnizorul va asigura remedierea oricărei deficiențe identificate în exploatare, pe cheltuiala acestuia.

19.3.2 Suport tehnic de 5 ani de la darea în exploatare pentru componentele software

Furnizorul trebuie să includă în oferta tehnică și servicii de suport tehnic aferente componentelor software ofertate, pe o perioadă de minim 5 ani de la data punerii în funcțiune. Suportul va fi oferit atât pentru produsele standard (COTS) cât și pentru cele dezvoltate în cadrul proiectului.
Pentru activitățile de suport tehnic, incidentele vor fi clasificate în mai multe categorii:

CRITIC

- Deranjamente care afectează activitatea instituțiilor din sistemul judiciar, determinând nefuncționarea sistemelor sau blocarea anumitor funcționalități.
- Aceste deranjamente afectează în mod direct serviciile furnizate, componente software cu impact asupra activității beneficiarului sunt inoperabile sau întregul sistem este inoperabil

MAJOR

- Problemele majore care au un impact semnificativ în funcționarea sistemelor și afectează în mod direct serviciile clienților. O componentă software este parțial inoperabilă având un impact major asupra activității beneficiarului. Aceste probleme nu sunt tolerate în folosința sistemelor.

MINOR

- Problemele minore care nu au un impact semnificativ în funcționarea sistemelor și nu afectează în mod direct serviciile clienților. O componentă software fără impact critic nu funcționează în parametri optimi. Aceste probleme sunt tolerate în folosința sistemelor.

Orar de preluare solicitări de intervenție, timp de răspuns și de remediere

- Orar: luni – vineri, orele 8 – 18 (excluzând sărbătorile naționale), considerate zile și ore lucrătoare.
- Pentru probleme critice (de severitate 1) care au ca efect oprirea funcționării sistemelor și/sau activității sau serviciilor instituției, ofertantul va oferi asistență permanentă, 24 x 24, 7 x 7, pe toata durata contractului.
- Timpul de răspuns la solicitările Autorității contractante reprezintă timpul de identificare a problemelor sesizate, chiar prin deplasare în locația de unde există acces la produsele/aplicațiile software care fac obiectul sesizării.
- Timpul de remediere a problemelor apărute în funcționarea sistemelor instalate sau în curs de instalare: (*Fix Time)* reprezintă durata de timp până la oferirea soluției finale.

Nivel de deranjament	Timp de răspuns	Timp de remediere
Critic	30 min	4 h
Major	1 h	8 h
Minor	4 h	2 zile

Nerespectarea orarului de preluare a solicitărilor, a timpilor de răspuns și/sau de remediere la solicitările Autorității contractante menționați mai sus, dă dreptul Autorității contractante de a percepe penalități și/sau a pretinde plata de daune-interese.

20. Licentiere produse software

Furnizorul va include in oferta licentele necesare pentru produsele implementate/utilizate care sa acopere inclusiv perioada de Garantie si Suport.