ITECHS S.R.L.

P R O P U N E R E T E H N I C Ă

Sistemul Informatic EVIDENCE

Dezvoltarea versiunii avansate — soluția tehnică, metodologia de implementare și angajamentele ofertantului

Autoritate contractantă	Inspectoratul General al Poliției al Republicii Moldova, IDNO 1013601000495
Procedură	Licitație deschisă nr. 21662736, lot nr. 12381954
Obiectul achiziției	Servicii de dezvoltare a softului „EVIDENCE” (versiunea avansată)
Document	Anexa nr. 23 — Propunerea tehnică
Ofertant	„ITECHS” S.R.L., IDNO 1013600030217, mun. Chișinău
Versiune	1.0 — 25 august 2026

Document înaintat în cadrul procedurii de achiziție publică, prin SIA RSAP.

Semnat electronic de reprezentantul legal al ofertantului.

Controlul documentului

Versiune	Data	Autor	Statut
0.9	23 august 2026	Echipa tehnică	Proiect intern, revizuit „patru ochi”
1.0	25 august 2026	Ion Prisacari, administrator	Versiune finală, depusă în SIA RSAP

Prezentul document constituie Propunerea tehnică depusă conform Anexei nr. 23 din documentația de atribuire. El se citește împreună cu Anexa T3 — Specificația logicii de business, document distinct, semnat electronic și depus în același dosar. Trimiterile interne de forma §N indică secțiuni din prezentul document; trimiterile de forma [CS §x, p.y] indică poziția corespunzătoare din Caietul de sarcini publicat de autoritatea contractantă.

Cuprins

Partea I — Cadrul ofertei

0. Datele ofertantului și declarația de conformitate

0.1 Identificarea ofertantului

Element	Valoare
Denumirea completă	Societatea cu Răspundere Limitată „ITECHS”
Denumirea prescurtată	„ITECHS” S.R.L.
Forma juridică de organizare	Societate cu răspundere limitată
IDNO / cod fiscal	1013600030217
Data înregistrării de stat	19 septembrie 2013
Sediul	MD-2044, str. Petru Zadnipru 1, ap. (of.) 52, mun. Chișinău, Republica Moldova
Reprezentant legal	Ion Prisacari, administrator, numit în funcție pe termen nelimitat
Beneficiar efectiv	Ion Prisacari — cotă de 100% din capitalul social
Capital social	5 400 lei
Document justificativ	Extras din Registrul de stat al persoanelor juridice nr. 628880 din 16 ianuarie 2026, eliberat de Agenția Servicii Publice
Persoana de contact pentru procedură	*[nume, funcție, telefon, e-mail]*
Semnătura electronică	MoldSign, aplicată de administrator

Obiectul principal de activitate al ofertantului, înscris în Registrul de stat, include: consultații în domeniul sistemelor de calcul; realizarea de programe și consultanța în domeniul dat; prelucrarea datelor; activități legate de băncile de date; activități de testări și analize tehnice; precum și **serviciile de creare, implementare și de asigurare a funcționării sistemelor informaționale automatizate de importanță statală, inclusiv a produselor program**. Ultima poziție acoperă direct obiectul prezentei achiziții.

0.2 Declarația de conformitate

Prin prezenta propunere tehnică, „ITECHS" S.R.L. declară că:

1. A studiat integral documentația de atribuire — Caietul de sarcini (44 pagini), anunțul de participare nr. 21662736, documentația standard, precum și răspunsurile la solicitările de clarificare publicate de autoritatea contractantă la 4 și 5 august 2026 — și își asumă executarea integrală a obiectului achiziției, pentru întregul lot, fără oferte alternative.
2. Soluția ofertată corespunde tuturor cerințelor obligatorii din Caietul de sarcini. Modul concret de îndeplinire a fiecărei cerințe este documentat în Anexa T1 — Matricea de conformitate, cu trimitere la capitolul și pagina din caiet și la secțiunea din prezenta propunere. Delimitările din §2 privesc exclusiv elemente pe care Caietul de sarcini nu le solicită sau pe care le condiționează el însuși de disponibilitatea unor terți; ele nu restrâng nicio cerință obligatorie.
3. Soluția se construiește exclusiv pe componente open source cu licențe permisive sau compatibile, fără costuri de licențiere pentru beneficiar, la achiziție și pe durata exploatării. Inventarul complet este în Anexa T2 — Bill of materials.
4. La finalul contractului, beneficiarul deține toate drepturile asupra codului sursă, bazei de date, documentației și configurațiilor, conform cap. 8.3 din Caietul de sarcini.

5. Ofertantul își asumă disponibilitatea de a efectua ajustări tehnice timp de 2 ani după finalizarea contractului, conform cerinței din anunțul de participare.
6. Oferta este valabilă 90 de zile calendaristice de la data-limită de depunere.
7. Stack-ul tehnologic prezentat în §4.2 constituie **propunerea** ofertantului, nu o condiție a ofertei. Componentele soluției pot fi convenite împreună cu beneficiarul în Etapele I–II, în limitele opțiunilor admise de Caietul de sarcini și fără a afecta cerințele obligatorii; substituirea unei componente cu una echivalentă funcțional nu modifică prețul.

0.3 Ce depune ofertantul, în plus față de minimul cerut

Caietul de sarcini descrie cele 14 module funcționale pe aproximativ 4 pagini, la nivel de intenție funcțională. O propunere tehnică formulată la același nivel de generalitate ar reproduce enunțurile caietului fără a demonstra că ofertantul le-a înțeles operativ.

De aceea, oferta include, ca Anexa T3, un document distinct — *Specificația logicii de business a Sistemului Informatic EVIDENCE, versiunea avansată* — care reconstruiește, la nivel implementabil:

- **actorii și cele trei niveluri de autorizare** (permisiune de acțiune, vizibilitate pe înregistrări, drepturi pe câmp × stare);
- **entitățile, atributele și constrângerile de integritate** pentru toate cele 14 module, plus funcționalitatea existentă care trebuie portată;
- **mașinile de stare** — stările, tranzițiile, gărzile și efectele lor;
- catalogul consolidat al regulilor de business, al regulilor de validare și al regulilor de afișare condiționată, fiecare cu identificator stabil;
- **criteriile de acceptanță** pe fiecare modul, formulate testabil;
- **matricea de trasabilitate** Caiet de sarcini → secțiune, pagină cu pagină;
- lacunele, ambiguitățile și contradicțiile identificate în Caietul de sarcini, cu poziția asumată de ofertant până la clarificarea lor comună în Etapa I.

Documentul folosește o convenție explicită de marcare a surselor: [CS §x, p.y] pentru cerințele formulate în caiet, [AS-IS §4.2, p.y] pentru comportamentul sistemului actual care trebuie portat, [PROP] pentru proiectarea propusă de ofertant, [CLARIF] pentru punctele care necesită decizie comună. Nicio afirmație marcată [CS] sau [AS-IS] nu extinde, restrânge sau reinterpretează textul caietului.

Scopul acestei anexe este dublu: să demonstreze comisiei nivelul real de înțelegere a domeniului și să constituie baza modelului TO-BE care va fi formalizat și aprobat în Etapa I, conform cap. 7.2, pct. 1 (p. 42) din Caietul de sarcini.

Anexa T3 se depune ca document distinct, semnat electronic, parte integrantă a prezentei propuneri tehnice. Trimiterile din matricea de conformitate (Anexa T1) către capitolele și anexele ei sunt verificabile direct în documentul depus.

0.4 Prototipul funcțional realizat de ofertant

Ofertantul a construit, înainte de semnarea contractului și pe baza specificației din Anexa T3, un prototip clicabil, funcțional în browser, disponibil pentru demonstrație la cererea autorității contractante. Prototipul are două componente:

Componentă	Ce demonstrează	Stadiu
Aplicația de back-office	Tabloul de bord SLA, fișa pachetului cu lanțul de custodie, registrul expertizelor, jurnalul de audit probatoriu, administrarea regulilor de formular	Cinci ecrane construite integral; restul modulelor sunt schițate ca structură de navigare

Componentă	Ce demonstrează	Stadiu
Aplicația de teren	Lista activităților cu starea de sincronizare, ecranul de scanare a codurilor, starea dispozitivului și semantica de conflict la sincronizare	Trei ecrane construite integral

Prototipul nu este o machetă grafică: **regulile de business din Anexa T3 sunt vizibile în interfață**, cu identificatorii lor. Un evaluator poate deschide ecranul de audit și poate vedea o tentativă de modificare respinsă cu motivul politica de câmp interzice, sau ecranul de administrare unde regula RD-CFL-003 face obligatoriu marcajul CIN pentru faptele enumerate în caiet.

Capturile din acest document provin din prototip. Ele poartă în subsol marcajul **„PROTOTIP · DATE DE DEMONSTRAȚIE"**: datele afișate sunt fictive, iar structura și denumirile reale se stabilesc de comun acord în Etapa I. Prototipul demonstrează mecanismele, nu conținutul.

Aceasta este poziția ofertantului față de cerința de la cap. 7.2, pct. 2 din Caietul de sarcini: **prototipurile UI/UX nu încep de la pagina albă în Etapa II**, ci de la un artefact deja construit, pe care beneficiarul îl poate critica și corecta din prima săptămână.

1. Înțelegerea obiectului achiziției

1.1 Nu este o dezvoltare de la zero

Prin clarificarea publicată la 5 august 2026, autoritatea contractantă a confirmat că ofertantul câștigător primește codul sursă al aplicației actuale (.NET), aplicația în funcțiune, structura bazei de date, ghidul utilizatorului și datele existente.

Aceasta schimbă natura proiectului. EVIDENCE a fost construit în 2020–2022, în cadrul proiectului transfrontalier România–Moldova (ENI 2SOFT/4.3/142), și este în exploatare la structurile criminalistice ale IGP. Obiectul achiziției este rescrierea și extinderea unui sistem viu, cu date de producție și cu utilizatori care lucrează zilnic în el — nu construirea unui produs nou.

Consecințele pe care ofertantul le-a integrat în proiectare:

Consecință	Cum o tratează oferta
Comportamentul actual este cerință contractuală, nu context	Cele 30 de pagini din cap. 4.2 sunt tratate ca specificație funcțională fermă. Fiecare regulă din ele apare, cu identificator, în Anexa T3.
Utilizatorii au deprinderi formate	Ecranele-cheie păstrează logica de lucru existentă; schimbările de interfață se justifică individual în prototipurile din Etapa II.
Datele existente trebuie să supraviețuiască	Migrarea are tratament propriu (§10), deși Caietul de sarcini nu o abordează — este subiectul unei clarificări asumate.
Codul .NET moștenit este o sursă de adevăr	În Etapa I, modelul AS-IS se construiește din caiet **și** din codul și schema primite, nu doar din documentație.

1.2 Asimetria Caietului de sarcini și ce înseamnă ea contractual

Caietul de sarcini are o structură asimetrică, pe care ofertantul o semnalează explicit pentru că determină modul de execuție:

- **circa 30 din 44 de pagini (cap. 4.2, p. 5–36)** descriu în detaliu comportamentul sistemului actual — câmpuri, validări, dinamica formularelor, reguli de custodie, segregarea pe roluri;
- cele 14 module funcționale ocupă circa 4 pagini (cap. 5, p. 36–40), la nivel de intenție funcțională, fără câmpuri, stări, ecrane sau criterii de acceptanță.

Asimetria nu este un defect al documentației, ci o caracteristică a proiectului, care trebuie gestionată contractual. Specificația reală a celor 14 module se formează în Etapa I. Mecanismul care protejează ambele părți este acceptarea formală a modelului TO-BE ca bază de referință contractuală la finalul Etapei I — pentru beneficiar, garanția că primește exact ce a descris; pentru prestator, protecția împotriva extinderii nelimitate a scopului într-un contract cu termen fix.

Anexa T3 este contribuția ofertantului la reducerea acestui risc înainte de semnarea contractului: modelul TO-BE nu pornește de la pagina albă în prima săptămână a Etapei I, ci de la un document deja structurat, care poate fi discutat, corectat și aprobat în workshopuri.

1.3 Ce acoperă sistemul actual și ce se adaugă

Portat integral [AS-IS §4.2]:

- **C.F.L.** — cercetarea la fața locului: înregistrarea activității, echipa, fapta, locul comiterii și locul desfășurării, urmele pe categorii, plicurile cu coduri de bare, planșa foto, finalizarea;
- **Expertize** — fluxul complet înregistrare → repartizare → examinare → finalizare → validare → expediere, inclusiv lucrările divizate, repetate, suplimentare și în comisie;
- **Administrare** — unități și subunități, funcții, grade, utilizatori, autoturisme, localități și străzi, fapte, moduri de operare, locuri de comitere, intervale de lucru, zile libere (inclusiv adăugarea automată a weekendurilor și normalizarea numelui de utilizator);
- **Statistici CFL** — funcționale în sistemul actual; statistica pe expertize, marcată „pagină în lucru", se finalizează.

Adăugat [CS §5] — șapte domenii operaționale noi: AUP și temeiuri legale; acțiuni tehnico-explozive (EOD); trageri experimentale și marcarea armelor; urme papilare și integrare AFIS; custodie și probe ca modul de sine stătător; corespondență și flux documentar; forensic intelligence și clasificări. Plus un strat de guvernanță a datelor: nomenclatoare versionate cu ferestre de valabilitate, reguli de formular per context, politici SLA, aprobări „patru ochi".

1.4 Cele patru cerințe care decid calitatea sistemului

Patru cerințe din documentație nu se rezolvă cu niciun produs sau framework existent. Ele reprezintă conținutul tehnic real al proiectului. Oferta le tratează ca priorități de arhitectură, nu ca funcționalități între altele:

1. **Autorizare granulară pe câmp × stare × rol** [CS §6.2, p. 40] — nu „ce module vede rolul", ci „ce câmp are voie să atingă, în ce stare a fluxului". Regula centrală a sistemului actual — *niciun rol nu poate modifica datele introduse de alt nivel* — este imposibil de respectat fără acest mecanism.
2. **Jurnal de audit inviolabil** [CS §5/M1, M13; §6.5, p. 41] — criptat, cu lanț de integritate verificabil, în care nici administratorul bazei de date nu poate modifica retroactiv un eveniment fără ca modificarea să devină detectabilă.
3. **Lanțul de custodie** [AS-IS §4.2; CS §5/M7] — mecanismul central al valorii probatorii, cu identificarea automată a incongruențelor.
4. **Lucrul offline în teren și reconcilierea** [CS §5/M2; §6.2] — cel mai mare bloc de risc tehnic al proiectului, care începe în Etapa II, nu în Etapa III.

Restul sistemului — oricât de întins — este muncă previzibilă. Aceste patru cerințe sunt cele pe care se pierde sau se câștigă recepția.

2. Delimitarea scopului ofertei

Pentru a evita orice ambiguitate la evaluare și la recepție, ofertantul delimitează explicit ce este inclus în preț.

2.1 Integrările cu sistemele criminalistice externe

Caietul de sarcini formulează integrarea cu EVOFINDER, TRAFFIC și AFIS în două trepte (cap. 5/M5, M6, p. 37–38 și cap. 6.4, p. 41), conectorii efectivi fiind condiționați de faptul că *„producătorii pun la dispoziție astfel de interfețe"*.

Delimitarea este respectată strict:

Element	Inclus în preț	Condiționat
Identificatorul extern ca atribut de primă clasă, cu validare de format, unicitate și jurnalizarea fiecărei modificări	**Da**	—
Arhitectura conectorului: interfața comună, contractul de date, maparea câmp-la-câmp, evenimentele create/update/delete, tratarea erorilor, reconcilierea, arhivarea schimburilor	**Da**	—
Serviciul intern de împachetare ANSI/NIST-ITL 1-2011 pentru AFIS (Type-1/2/9/13/14), cu codare WSQ	**Da**	—
Activarea efectivă a unui conector către un sistem terț	—	**Da** — condiționat de existența, documentarea și accesul la API-ul producătorului, precum și de acordurile de interoperabilitate dintre instituții
Algoritmi proprii de comparare biometrică sau balistică	Caietul nu îi solicită: cap. 5/M5, M6 și cap. 6.4 definesc corelarea prin **identificator extern** și prin conectori, ambele integral incluse	—

Această delimitare protejează ambele părți: beneficiarul primește tot ce depinde de prestator, iar prestatorul nu răspunde pentru disponibilitatea unor interfețe controlate de terți.

2.2 Integrarea cu platformele guvernamentale

Cap. 6.2 (p. 40–41) prevede explicit că integrarea cu MPass este opțională, *„fără a condiționa funcționarea sistemului de această integrare"*, iar semnarea se poate face *„fie prin servicii externe dedicate, precum MSign, fie prin mecanisme interne de validare și asumare"*. Cap. 5 (modulele 1, 4, 9, 12) tratează însă integrarea ca dată.

Poziția ofertantului: sistemul se livrează cu ambele variante implementate și comutabile din configurație:

- autentificare locală completă (politici de complexitate, expirare, blocare, MFA prin TOTP) — deci cerința de autentificare multifactor este satisfăcută independent de MPass;
- schema externă MPass (SAML), activabilă din configurație, cu provisioning just-in-time pe IDNP;
- semnare prin MSign, cu marcă temporală calificată;
- mecanism intern de asumare și validare, cu dovezi de integritate, pentru cazurile în care MSign nu este disponibil.

Costul acestei duble implementări este asumat de ofertant. Beneficiul pentru beneficiar: sistemul intră în producție la termen chiar dacă formalitățile de conectare la AGE (Formularul Unic de Conectare, certificatul de sistem de la STISC, accesul la mediile de staging) întârzie.

2.3 Ce nu conține prezenta propunere

– **Estimări de efort, prețuri sau grafice de resurse financiare** — acestea sunt în Propunerea financiară (Anexa nr. 22).

– **Furnizarea de echipamente** — imprimante mobile de etichete, scanere, tablete, servere. Sistemul este proiectat să funcționeze cu echipamentele beneficiarului; specificațiile de compatibilitate se stabilesc în Etapa I.

– **Găzduirea** — soluția se livrează pentru rulare pe MCloud, sub administrarea tehnică STISC, conform principiilor AGE. Costurile de infrastructură MCloud nu fac obiectul prezentei oferte. Angajamentele de disponibilitate și de restaurare din §9 sunt asumate pentru configurația de infrastructură dimensionată în Etapa II și pusă la dispoziție de beneficiar — replici multiple ale serviciului, bază de date în configurație de înaltă disponibilitate, spațiu de backup în două locații. Dimensionarea se stabilește și se acceptă în scris la finalul Etapei II, astfel încât ambele părți să știe exact ce susține pragul de 99,5%.

Partea II — Soluția tehnică

3. Principiile de proiectare

Cinci principii guvernează întreaga soluție. Ele nu sunt declarații de intenție: fiecare se materializează într-un mecanism verificabil la recepție.

#	Principiu	Materializare	Verificabil prin
P1	Ceea ce s-a întâmplat nu se rescrie	Activitățile CFL finalizate și expertizele validate nu se șterg; corecțiile se fac prin acte noi, legate de cele vechi; jurnalul probatoriu este append-only, protejat la nivel de bază de date	CA-* din Anexa T3; test de tentativă de ștergere pe fiecare stare finală
P2	Fiecare atingere a unei probe lasă urmă	Fiecare mișcare de pachet produce un eveniment de custodie cu custode, moment, loc și semnătură; incongruențele se semnalează automat	Reconstituirea completă a traseului oricărui pachet, la cerere
P3	Niciun rol nu modifică datele altui nivel	Matricea FieldPolicy (rol × entitate × stare × câmp), evaluată la fiecare citire și la fiecare scriere	Anexa D din T3 — matricea drepturilor; teste automate pe fiecare celulă
P4	Regulile de business sunt date, nu cod	Mașinile de stare, politicile SLA, regulile de formular, nomenclatoarele și matricea de drepturi se administrează din interfață, cu versionare și aprobare „patru ochi"	Modificarea unei politici SLA fără redeploy, demonstrată la UAT
P5	Fiecare afirmație are o dovadă	Integritatea auditului se demonstrează printr-un raport de verificare, nu prin declarație; integrarea condiționată de terți este marcată ca atare; lacunele caietului sunt declarate și tratate, nu acoperite cu formulări generale	Anexa F din T3 — lacunele identificate, cu poziția asumată

4. Arhitectura sistemului

4.1 Conformitatea cu cerințele arhitecturale din caiet

Cerință [CS §6.1, p. 40]	Soluția ofertată
Model **3-tier** — interfață, logică de business, strat de date, cu separare strictă	Frontend React (SPA + PWA) · Backend ASP.NET Core cu straturi Domain / Application / Infrastructure separate fizic în proiecte distincte · PostgreSQL. Fiecare strat este testabil independent.
Comunicare prin **servicii RESTful JSON**	API REST/JSON documentat OpenAPI, generat din application services; clientul TypeScript se generează din specificația OpenAPI la fiecare build
HTTPS / TLS 1.3	TLS 1.3 obligatoriu, HSTS, CSP strictă fără unsafe-inline
100% web-based, fără instalare locală	SPA pentru back-office, PWA pentru teren — ambele rulate din browser, fără instalare
Chrome, Edge, **Firefox**; rezoluții variate, tablete și laptopuri	Suport complet pe toate cele trei browsere. Excepția tehnică pentru tipărirea etichetelor pe imprimante Bluetooth este tratată în §7.4
Platformă enterprise: **.NET 8 / Java EE / Python FastAPI**	ASP.NET Core, pe .NET 8 — versiunea nominalizată în caiet. Trecerea la o versiune LTS superioară se face numai cu acordul beneficiarului, în Etapa II

Cerință [CS §6.1, p. 40]	Soluția ofertată
SGBD relațional cu **proceduri stocate și integritate referențială**	**PostgreSQL** + PostGIS. Chei străine reale pe toate relațiile, constrângeri UNIQUE, CHECK și EXCLUDE, proceduri stocate acolo unde sunt justificate (§4.4)
Open source, fără costuri adiționale de licențe	Întregul stack — Anexa T2. Nicio componentă cu licență comercială, la achiziție sau în exploatare

4.2 Stack-ul tehnologic

Strat	Tehnologie	Licență
Frontend back-office	React + TypeScript + Vite, Refine, TanStack Query, MUI	MIT
Aplicație de teren	PWA: Workbox + IndexedDB (Dexie) + outbox propriu	MIT / Apache-2.0
Backend	ASP.NET Core + ABP Framework (ediția gratuită)	MIT / LGPL-3.0
ORM	Entity Framework Core	MIT
Bază de date	PostgreSQL	PostgreSQL License
Extensie geospațială	PostGIS	GPL-2.0 — extensie de bază de date, neîncorporată în aplicație
Cache și lock distribuit	Valkey sau Redis, la alegerea beneficiarului	BSD-3-Clause / AGPL-3.0*
Stocare obiect	SeaweedFS (API compatibil S3)	Apache-2.0
Identitate	OpenIddict + SDK oficial MPass SAML	Apache-2.0 / MIT
Semnătură	MSign prin SDK oficial; DSS pentru validare și conservare pe termen lung	MIT / LGPL-2.1
Chei criptografice	OpenBao (motor transit)	MPL-2.0
Generare PDF	Typst + Gotenberg	Apache-2.0 / MIT
Generare XLSX	ClosedXML	MIT
Grafice	Apache ECharts	Apache-2.0
Coduri de bare	ZXing.Net, BinaryKits.Zpl, Barcode Detection API	Apache-2.0 / MIT
Hărți	MapLibre GL JS	BSD-3-Clause
Calitatea imaginilor dactiloscopice	NFIQ 2, libbiomeval	domeniu public
Observabilitate	OpenTelemetry, Prometheus, Grafana, OpenSearch	Apache-2.0 / AGPL*
Rulare	Docker, Kubernetes, Helm — pe MCloud	Apache-2.0

* Componentele marcate cu asterisc — Grafana și, dacă beneficiarul o alege, Redis — rulează ca servicii separate, nemodificate, fără legare cu codul aplicației. Este cazul de utilizare permis explicit de licența AGPL-3.0, fără costuri și fără efect asupra drepturilor beneficiarului asupra codului sursă. Analiza completă a implicațiilor de licențiere este în Anexa T2.

Două alegeri merită justificate explicit, pentru că sunt puncte în care ofertele se diferențiază:

Cache-ul distribuit: Valkey sau Redis. Cele două produse vorbesc același protocol, iar aplicația nu le distinge: componenta se schimbă dintr-o linie de configurare, fără modificări de cod. Ambele sunt disponibile fără costuri de licențiere și ambele satisfac cerința din caiet. Diferența este de regim juridic, iar ofertantul o expune pentru ca beneficiarul să decidă în cunoștință de cauză:

Opțiune	Licență	Ce înseamnă practic	Când se recomandă
Valkey	BSD-3-Clause, permisivă	Fără nicio obligație de reciprocitate, indiferent cum este folosit. Fork al Redis aflat sub Linux Foundation, cu aceeași interfață	Varianta implicită propusă, pentru că este cea mai simplă de apărat într-un dosar de conformitate de licențiere
Redis	AGPL-3.0, copyleft	Fără costuri, cu condiția să ruleze ca serviciu separat și nemodificat — exact modul în care este folosit aici. Obligațiile AGPL s-ar activa doar dacă beneficiarul ar modifica Redis și ar oferi accesul unor terți	Dacă echipa IT a beneficiarului are deja Redis în exploatare și competențe formate pe el

Ofertantul propune Valkey ca variantă implicită și livrează soluția pregătită pentru ambele. Decizia se consemnează în Etapa II, ca decizie de arhitectură, și nu modifică prețul.

Ediția gratuită a ABP Framework, consumată prin NuGet, fără fork. Nu se folosesc modulele comerciale, tema comercială sau uneltele de generare cu plată. Interfața este dezvoltată în întregime de ofertant, în React, deci dependența de straturile UI comerciale ale framework-ului nu există. Acesta este un angajament ferm, verificabil în bill of materials și în fișierele de proiect livrate.

Stack-ul este o propunere supusă discuției, nu o condiție a ofertei

Tabelul de mai sus exprimă alegerea pe care ofertantul o consideră cea mai potrivită pentru cerințele acestui caiet, argumentată tehnic în secțiunile care urmează. **Ea nu este însă o condiție a ofertei.** Ofertantul este deschis să adapteze componentele soluției la preferințele, standardele interne și competențele existente ale beneficiarului, iar discuția pe acest subiect este binevenită încă din Etapa I.

Distincția care contează pentru evaluare:

Element	Statut
Cerințele din Caietul de sarcini — model 3-tier, REST/JSON, TLS 1.3, funcționare 100% web, SGBD relațional cu integritate referențială și proceduri stocate, componente open source fără costuri de licențe, securitatea, auditul, performanța și disponibilitatea din cap. 6	**Ferm.** Nu depind de alegerea componentelor și se respectă integral, indiferent de stack-ul convenit
Platforma de dezvoltare, în limitele opțiunilor acceptate de caiet (.NET 8 / Java EE / Python FastAPI)	**Deschis discuției**
Sistemul de gestiune a bazelor de date, în limitele opțiunilor acceptate de caiet	**Deschis discuției**, cu precizarea de la §20.2 privind costurile de licențiere
Componentele de infrastructură — cache distribuit, stocare de obiecte, motor de workflow, generare de documente, observabilitate, biblioteci de interfață	**Deschise discuției**, fiecare în parte

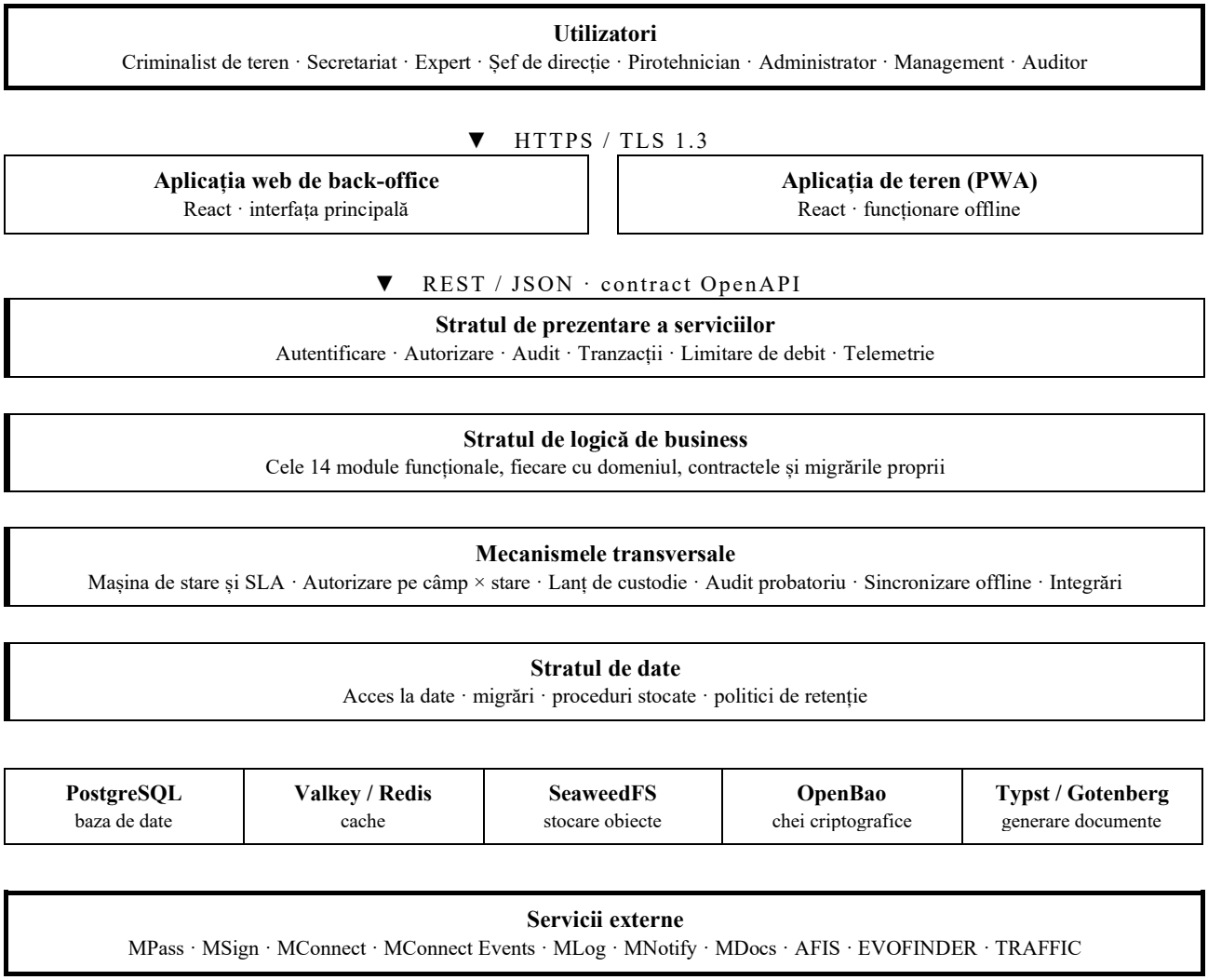
Această flexibilitate nu este o formulă de curtoazie: ea este posibilă pentru că **arhitectura izolează componentele de infrastructură în spatele unor contracte interne**. Cache-ul, stocarea de obiecte, generarea de documente sau motorul de workflow sunt consumate prin interfețe, nu direct din logica de business. Înlocuirea uneia dintre ele schimbă o implementare și o linie de configurare, nu regulile din Anexa T3. Exemplul din §4.2 — Valkey sau Redis — este tocmai ilustrarea acestui principiu.

Cum se decide, practic. Fiecare alegere de componentă se discută în Etapele I–II și se consemnează ca decizie de arhitectură (ADR), cu alternativele evaluate și motivul deciziei, astfel încât beneficiarul să știe nu doar *ce* s-a ales, ci și *de ce*. Substituirea unei componente cu una echivalentă funcțional **nu modifică prețul ofertei**. Dacă o preferință exprimată de beneficiar ar avea efect asupra efortului, a termenului sau a licențierii, ofertantul semnalează acest lucru înainte de decizie, cu impactul cuantificat — pentru ca alegerea să fie făcută în cunoștință de cauză, nu descoperită la recepție.

Singura rezervă pe care ofertantul o formulează explicit: **o componentă care ar introduce costuri de licențiere pentru beneficiar intră în contradicție cu cerința din Caietul de sarcini**, iar ofertantul are obligația să o semnaleze ca atare. În rest, decizia aparține beneficiarului.

4.3 Vedere de ansamblu

Figura 1. Vederea de ansamblu a soluției



Un singur deployabil pentru API, scalat orizontal. Procesele de fundal — timere SLA, sigilii de audit, sincronizări, reîmprospătarea agregărilor — rulează într-un serviciu separat din aceeași soluție, cu alegere de lider, pentru a evita execuțiile concurente.

Monolit modular, nu microservicii. Într-un contract cu 14 module și un interval de patru luni, costul operațional al unei arhitecturi distribuite (rețea, observabilitate distribuită, consistență eventuală, orchestrare) nu se amortizează. Modularitatea se obține la nivel de cod — fiecare modul cu straturile, migrările și spațiul său de nume, comunicând prin contracte explicite și evenimente de domeniu, niciodată prin acces direct la datele altui modul. Granițele sunt trasate astfel încât, dacă în viitor un modul trebuie extras într-un serviciu separat, extragerea să nu necesite rescriere.

Cerința de comunicare între module prin servicii RESTful JSON este îndeplinită în litera ei: fiecare modul își expune integral funcționalitatea printr-un API REST/JSON documentat în OpenAPI, cu rutare pe modul (api/evidence/<modul>/<resursă>), versionare și autorizare proprii. Interfața web, aplicația de teren și orice sistem extern consumă exclusiv aceste API-uri. Topologia de rulare — un singur proces sau procese separate — nu schimbă contractul de comunicare, ci doar costul de operare.

Această alegere satisface și principiul event-driven publicat de AGE: modulele emit evenimente de domeniu la fiecare modificare semnificativă, iar un subset filtrat al acestora se publică extern, în format CloudEvents, către MConnect Events.

4.4 Unde stau invarianții

Caietul cere „integritate referențială și proceduri stocate" [CS §6.1, p. 40]. Traducerea în trei niveluri, cu criteriul „regula trebuie să fie imposibil de încălcat, nu doar validată în interfață":

În schema bazei de date — chei străine reale pe toate relațiile; UNIQUE pe numărul de înregistrare al expertizei la nivel național — extinderea cerută de M8 față de unicitatea actuală pe an și unitate —, pe codul de bare, pe (funcție, perioadă de ocupare); CHECK pentru „data activității nu poate fi în viitor", „durata nu poate depăși intervalul", „aprobatorul nu poate fi identic cu inițiatorul"; indecși parțiali pentru cozile de lucru și termenele scadente; constrângere de excludere pe intervale, pentru a garanta că o funcție are un singur ocupant la un moment dat.

În proceduri stocate — pentru operațiunile care trebuie garantate la nivelul bazei de date, indiferent de aplicația care le apelează: generarea atomică a numerelor de ordine (ID caz CFL, număr de înregistrare a expertizei) sub blocare consultativă, pentru a exclude condițiile de cursă la concurență; verificarea lanțului de audit; agregările grele pentru tablourile de bord.

În stratul de domeniu — regulile care depind de rol, stare și context: cine poate trece o lucrare dintr-o stare în alta, ce câmpuri se activează la marcajul PIN, când devine obligatorie conexarea cu un caz existent. Aici sunt testabile automat, ceea ce în proceduri stocate nu ar fi.

Anexa B din T3 listează separat regulile a căror încălcare este imposibilă prin construcție — cele garantate la nivel de bază de date. Este lista pe care o verifică un evaluator tehnic pentru a distinge o validare reală de una cosmetică.

5. Cele 14 module funcționale

Fiecare modul din cap. 5 al Caietului de sarcini corespunde unui modul de cod independent, cu straturile și migrările proprii.

Modul	Denumire (caiet)	Modul de cod	Depinde de
M1	Utilizatori, Identitate și Semnătură	Identity	Administration
M2	CFL — Cercetare la Fața Locului	FieldWork	Custody, Administration
M3	AUP și Temeiuri Legale	Prosecution	FieldWork
M4	Acțiuni Tehnico-Explozive (EOD)	Eod	Custody
M5	Trageri Experimentale și Marcarea Armelor	Ballistics	Custody
M6	Urme Papilare și Integrare AFIS	Dactyloscopy	Custody
M7	Custodie și Probe	Custody	Administration
M8	Registrul Digital al Expertizelor	Forensics	Custody, Workflow
M9	Corespondență și Flux Documentar	Correspondence	Administration
M10	Interoperabilitate și Conectori	Interop	toate
M11	Forensic Intelligence și Clasificări	Intelligence	toate
M12	Rapoarte și Analitică	Reporting	toate
M13	Calitate și Audit	Quality	Auditing

Modul	Denumire (caiet)	Modul de cod	Depinde de
M14	Administrare, Nomenclatoare și Configurații	Administration	—

Plus trei module de infrastructură, transversale, care nu apar ca module funcționale în caiet dar sunt cerute implicit de el: Workflow (mașina de stare și SLA), Auditing (jurnalul probatoriu), Sync (protocolul offline).

Pentru fiecare modul, Anexa T3 conține: domeniul funcțional, actorii și drepturile lor, entitățile cu atributele și constrângerile, stările și tranzițiile, regulile de business cu identificator, politicile SLA, ecranele și criteriile de acceptanță. Rezumatul de mai jos indică doar elementul care definește fiecare modul.

M1 — Utilizatori, Identitate și Semnătură. Autentificare locală cu MFA sau prin MPass, la alegerea beneficiarului. Cele trei niveluri de autorizare. Dosarele de personal cu licențele de expertiză și ferestrele lor de valabilitate — o licență expirată blochează automat repartizarea lucrărilor din specialitatea respectivă. Semnarea prin MSign sau prin mecanism intern.

M2 — CFL. Modulul cu cea mai mare încărcătură de reguli existente și singurul care funcționează offline. Flux pe pași, geolocație și timp captate automat, generarea și tipărirea etichetelor în teren, planșa foto, monitorizarea timpilor pe etape. Întreaga dinamică a formularului din sistemul actual — „la sediu", PIN, CIN, reluare/continuare, conexări obligatorii — este catalogată ca reguli RD-CFL-* în Anexa T3.

M3 — AUP și Temeiuri Legale. Repertoriul codificat al infracțiunilor și registrul temeiurilor (ordonanțe, solicitări, demersuri), care guvernează dinamica formularelor: temeiul determină ce câmpuri devin obligatorii. Legături cauză–act–persoane–obiecte, SLA pe stadii.

M4 — EOD. Taxonomii de dispozitive și niveluri de risc, flux notificare → dislocare → intervenție → raport, ancorare probatorie foto/video, evidența autospecialelor și a echipamentelor de intervenție alocate fiecărei dislocări, acces segregat pe profiluri — datele EOD nu sunt vizibile implicit celorlalte structuri.

M5 — Trageri experimentale și marcarea armelor. Trasabilitate de la recepția armei la rezultatul balistic, caracteristici tehnice, loturi de tragere, identificator extern pentru EVOFINDER/TRAFFIC, rapoarte semnate electronic.

M6 — Urme papilare și AFIS. Ciclul complet prelevare → evaluare calitativă (NFIQ 2) → prelucrare → transmitere → recepție rezultat → arhivare, cu metadate standardizate per urmă și SLA pe fiecare etapă. Fiecare urmă rămâne corelată cu dosarul, locul, obiectul purtător și, după identificare, cu persoana — legături care alimentează direct analiza de serii și patternuri din M11. Serviciul intern de împachetare ANSI/NIST-ITL construiește tranzacțiile în formatul standard, independent de existența unui conector activ.

M7 — Custodie și Probe. Modulul care transformă lanțul de custodie din comportament difuz în entitate de sine stătătoare. Coduri Data Matrix, imprimante mobile, înregistrarea fiecărei mișcări, semnalarea automată a incongruențelor, versionarea concluziilor, examinări complexe și în comisie.

M8 — Registrul Digital al Expertizelor. Numerotare automată națională, cu prefixe configurabile (an, unitate, segment) — extindere față de numerotarea actuală, unică pe an și unitate. Fluxul complet, arhivarea rapoartelor și planșelor în PDF, export prin API cu filtrare pe drepturile solicitantului.

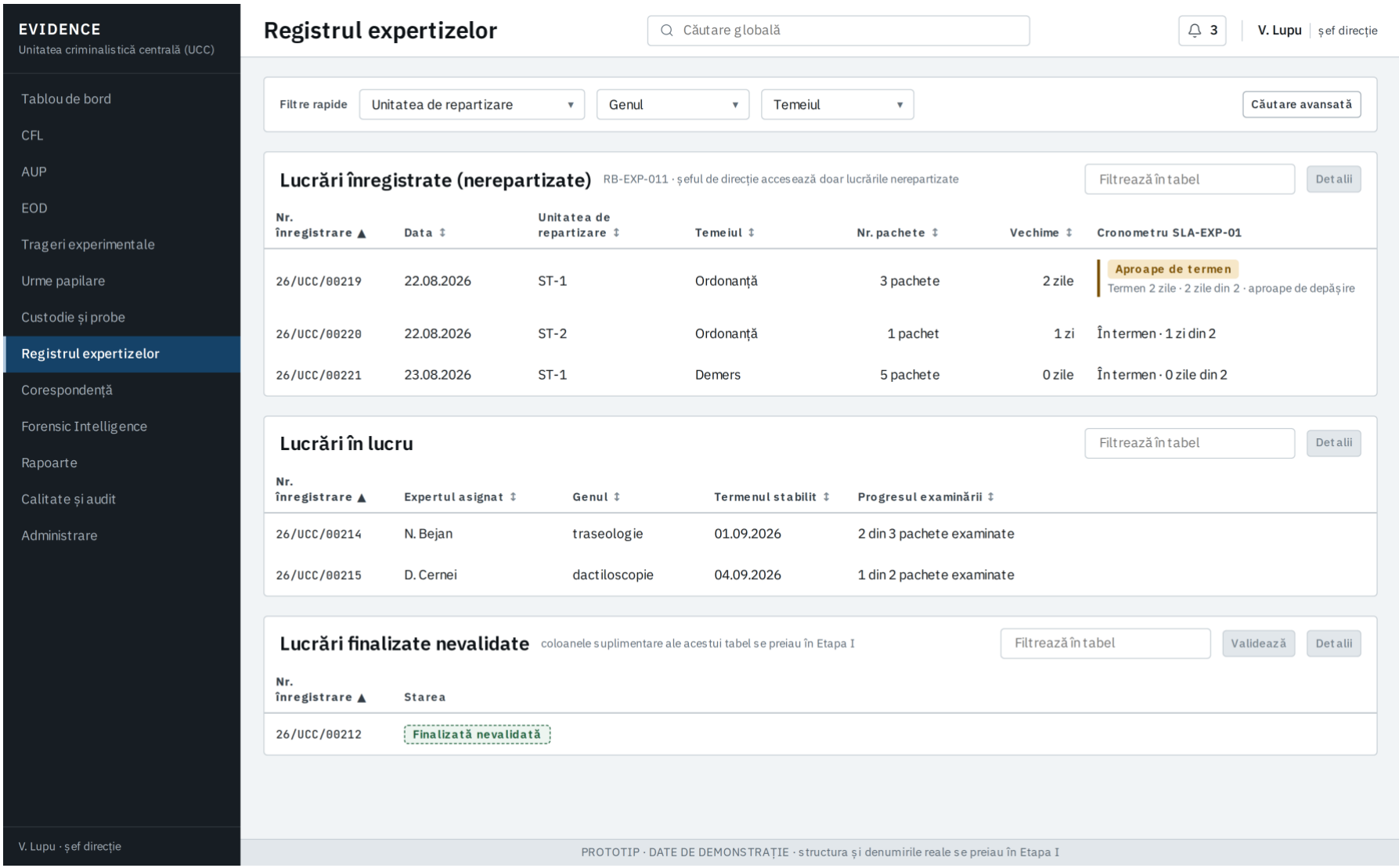


Figura 2. Registrul expertizelor, în prototip. Cele trei tabele corespund stărilor din mașina de stare a lucrării: înregistrată și nerepartizată, în lucru, finalizată nevalidată. Coloana din dreapta afișează cronometrul SLA-EXP-01 (intrare → alocare) pentru fiecare lucrare, cu marcajul „Aproape de termen" la două zile din două. Textul de lângă titlu citează regula RB-EXP-011, care limitează accesul șefului de direcție la lucrările nerepartizate.

M9 — Corespondență și Flux Documentar. Registrul intrărilor și ieșirilor, normalizarea metadatelor, semnare și contrasemnare, căutare inter-modulară, notificări de scadență.

M10 — Interoperabilitate și Conectori. Singurul modul care vorbește cu exteriorul. Contracte de date, mapări câmp-la-câmp, fluxuri de evenimente, rezolvarea conflictelor, jurnal inviolabil al schimburilor.

M11 — Forensic Intelligence și Clasificări. Taxonomie multi-criterială, identificarea de patternuri, serii și rute, rețele de corelații între cazuri, monitorizarea calității datelor. Modulul se construiește exclusiv pe datele pe care sistemul le colectează deja — nu presupune surse externe.

M12 — Rapoarte și Analitică. Patru familii: operaționale, statistice, de conformitate, de performanță. Filtrare avansată, export PDF/XLSX, semnare electronică a rapoartelor oficiale. Include finalizarea statisticii pe expertize, marcată „pagină în lucru" în sistemul actual.

M13 — Calitate și Audit. Controale automate în punctele critice ale fluxurilor, jurnale read-only protejate criptografic, rate de respingere, timpi de reverificare.

M14 — Administrare, Nomenclatoare și Configurații. Registrul centralizat de taxonomii cu versionare și ferestre de valabilitate — cerință care schimbă modelul de date, nu doar interfața: un raport pe 2024 trebuie să afișeze denumirea unității așa cum era în 2024. Plus regulile de formular per context, șabloanele, politicile SLA și aprobările „patru ochi".

6. Mecanismele transversale

Zece mecanisme traversează toate modulele. Ele sunt partea din sistem care nu se vede în lista de funcționalități, dar care determină dacă rezultatul este un sistem probatoriu sau o colecție de formulare.

6.1 Identificatori, numerotare și unicitate

ID-ul de caz CFL se generează la salvare din abrevierea raionului, ultimele două cifre ale anului și un număr de ordine incremental, și nu se mai schimbă niciodată. Numărul de înregistrare al expertizei devine unic la nivel național, cu prefixe configurabile. Numărul unic de caz are 10–12 cifre, cu respingerea duplicatelor. Un cod de bare nu se reutilizează și nu poate aparține simultan la două lucrări. O funcție are un singur ocupant la un moment dat.

Generarea numerelor se face atomic, sub blocare consultativă în baza de date — nu în cod de aplicație. Este singura variantă care rezistă la salvări concurente din două unități, iar acceptanța include un test de concurență explicit (CA-EXP-001).

6.2 Consistență temporală și calendarul de lucru

Regulile existente se păstrează integral: data activității nu poate fi în viitor și nu poate preceda data comiterii faptei; durata nu poate depăși intervalul dintre ora de început și cea de sfârșit; dacă ora finală este mai mică decât cea inițială, data finală avansează automat cu o zi; căutarea pe interval se face pe criteriul suprapunerii cu cel puțin o zi.

Extindere necesară: odată introduse SLA-urile, calendarul de lucru devine structură de prim rang. Un termen de „48 de ore" nu înseamnă același lucru vineri seara și marți dimineața. Intervalele de lucru și zilele libere legale sunt deja nomenclatoare în sistemul actual — soluția le promovează la rangul de calendar de referință folosit de motorul de termene.

6.3 Motorul de reguli de formular

Dinamica formularelor din sistemul actual nu este o colecție de particularități de interfață: este logică juridică integrată în ecran. „La sediu" ascunde câmpurile de deplasare pentru că, juridic, nu există deplasare. PIN lasă active doar Data găsirii și Descrierea cazului pentru că, până la identificare, restul datelor nu există

legal. CIN se activează automat pentru omor, moarte subită, accident cu victime, accident cu părăsirea locului.

Soluția tratează aceste reguli ca date configurabile, nu ca ramificații în cod: fiecare regulă are declanșator, condiție, efect (arată / ascunde / activează / dezactivează / face obligatoriu / precompletează) și domeniu de aplicare. Catalogul complet al regulilor existente este în Anexa T3, cu identificatori RD-*. Mecanismul se extinde direct la modulele noi — în special M3, unde temeiul legal determină câmpurile obligatorii.

Beneficiul operațional: adăugarea unui nou tip de faptă cu propriile câmpuri obligatorii se face din administrare, nu printr-o versiune nouă de software.

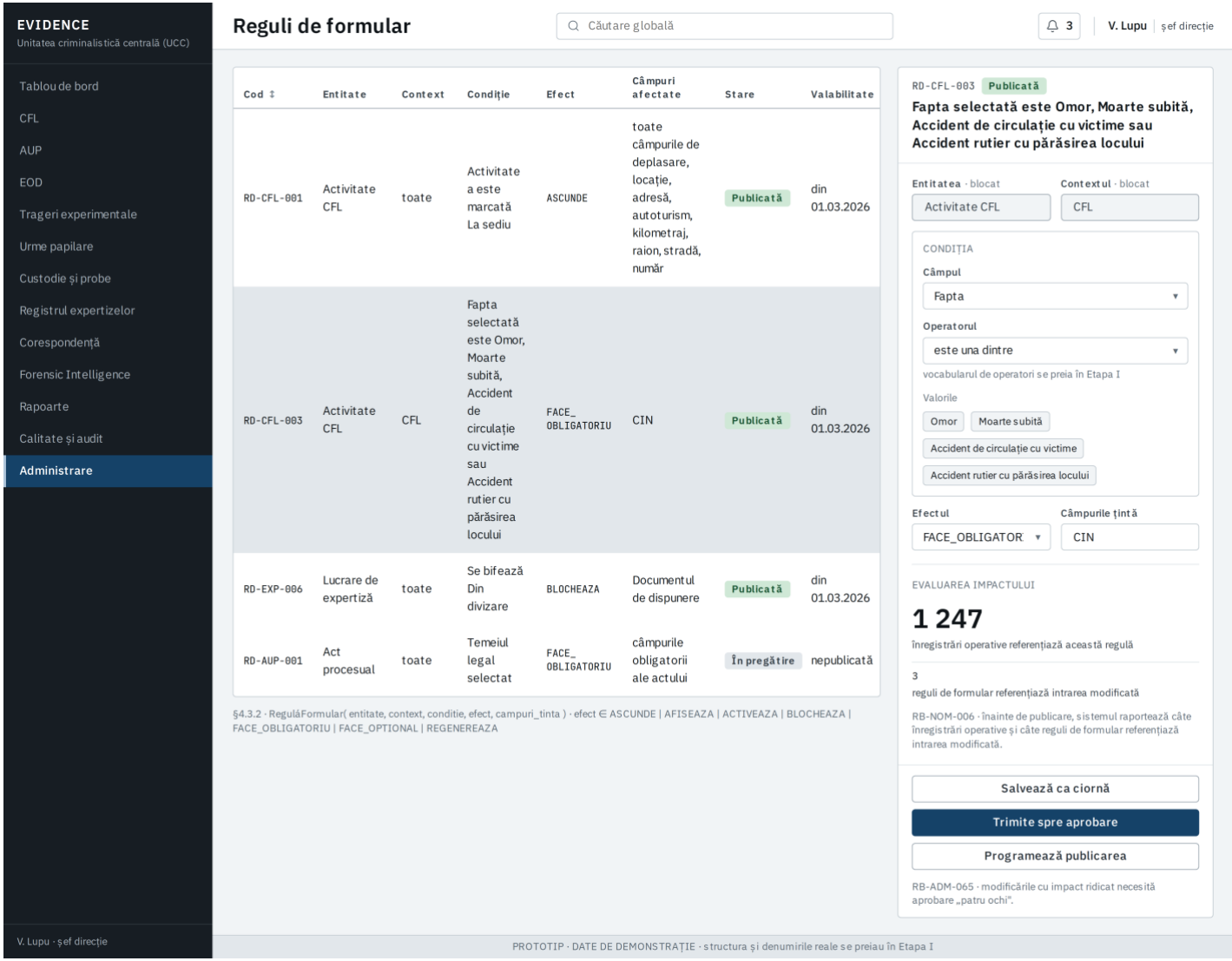


Figura 3. Administrarea regulilor de formular. Fiecare regulă are cod, entitate, context, condiție, efect și câmpuri afectate, iar starea „Publicată" o separă de cea „În pregătire". În dreapta, editorul regulii RD-CFL-003: fapta selectată dintre Omor, Moarte subită, Accident de circulație cu victime sau Accident rutier cu părăsirea locului face obligatoriu marcajul CIN. Panoul de evaluare a impactului arată câte înregistrări operative referențiază regula înainte de publicare.

6.4 Lanțul de custodie

Pachet este agregatul central, cu identificator unic generat pe server (prefix instituțional + secvență + cifră de control) și materializat ca Data Matrix ECC200, care rămâne lizibil cu circa 30% din suprafață deteriorată — relevant pentru etichete aplicate pe ambalaje manipulate în teren.

Fiecare atingere a pachetului produce un eveniment de custodie: ridicare, transport, predare, preluare, depozitare, examinare, returnare, arhivare — cu custode, moment, loc și semnătură. Sistemul semnalează automat incongruențele: două predări consecutive fără preluare intermediară, un pachet scanat în două locuri la momente incompatibile, o mișcare înregistrată retroactiv.

Regulile din sistemul actual se păstrează integral: scanarea obligatorie a codului la fiecare plic din CFL; modificarea numărului de plicuri regenerează structura de câmpuri; un cod scanat care nu aparține lucrării repartizate blochează examinarea; pachetele nu se mută după începerea examinării și nu se elimină dintr-o lucrare divizată; în lucrările divizate, pachetele alocate se afișează pe fond negru, cele nealocate pe gri.

Rezultatul verificabil la recepție: pentru orice pachet, la orice moment, sistemul reconstituie traseul complet, cu răspunzător pe fiecare segment.

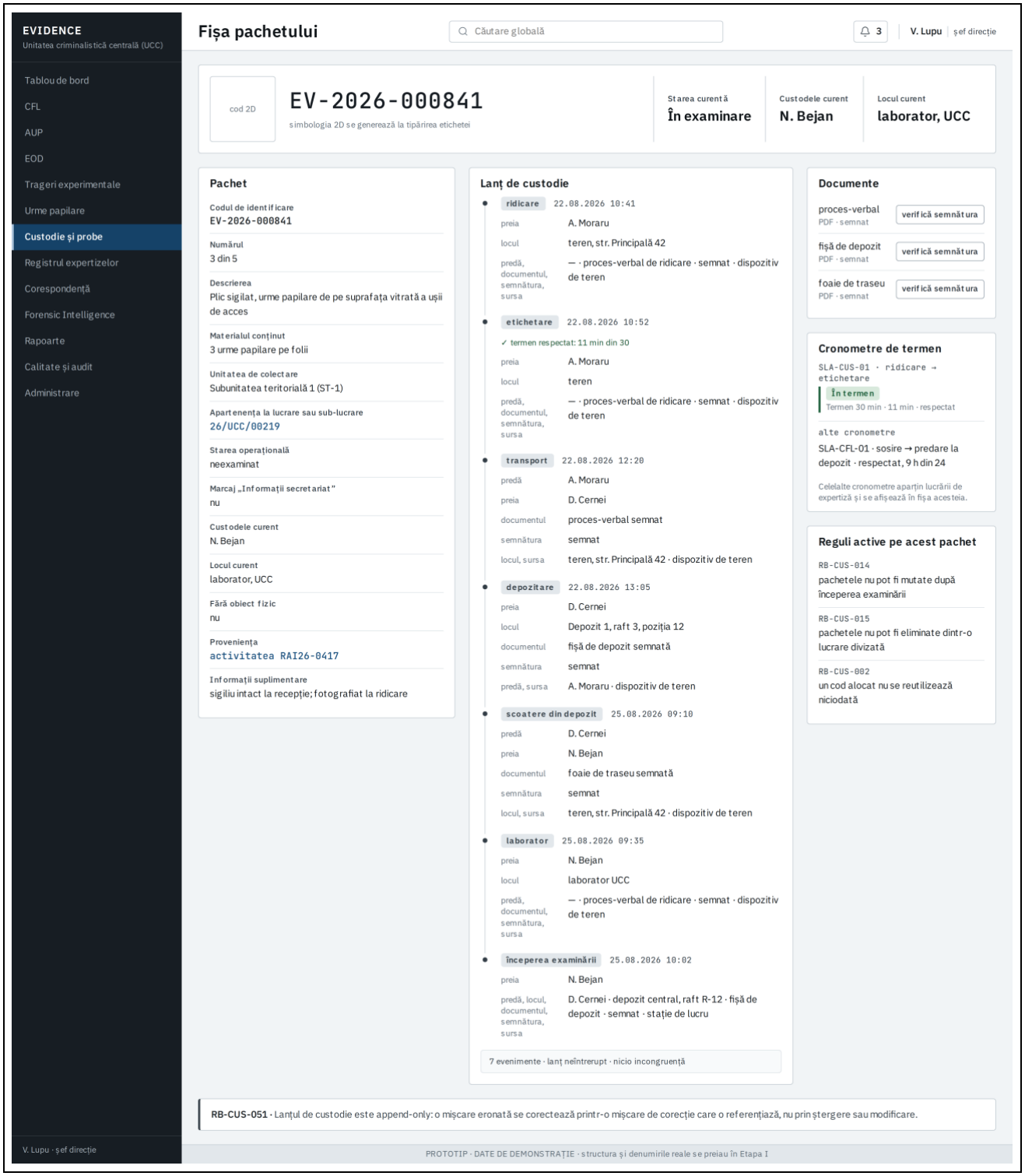


Figura 4. Fișa pachetului EV-2026-000841. Coloana centrală reconstituie lanțul de custodie eveniment cu eveniment — ridicare, etichetare, transport, depozitare — cu cine predă, cine preia, locul, documentul și semnătura. Etichetarea afișează termenul respectat: 11 minute din 30, adică politica SLA-CUS-01. Panoul din dreapta enumeră regulile active pe pachet, printre care RB-CUS-014: pachetele nu pot fi mutate după începerea examinării.

6.5 Mașina de stare și politicile SLA

Caietul cere SLA-uri configurabile pe fiecare pas de flux, cu praguri stabilite de management, alerte la depășire și agregare în tablouri de bord [CS §5/M2, M3, M6, M12]. Aceasta nu este o funcționalitate de raportare: presupune ca fiecare pas al fiecărui flux să fie o entitate identificabilă, cu moment de intrare, moment de ieșire și termen-țintă.

Structura propusă:

```
MașinăDeStare(tip entitate)
  Stare(cod, denumire, este finală, este arhivată)
  Tranziție(din stare, în stare, permisiune, gardă, efect)
PoliticăSLA(tip entitate, pas, tip expertiză?, prioritate?,
            durată-țintă, calendar)
CalendarDeLucru(intervale de lucru, zile libere legale)
```

La fiecare tranziție se calculează termenul pasului următor, folosind calendarul de lucru real. Un proces de fundal scanează termenele scadente și emite evenimente de depășire, traduse în notificări (MNotify sau canal intern). Tablourile de bord se alimentează din agregări reîmprospătate periodic, nu din interogări directe pe tabelele operative — aceasta este cea mai frecventă cauză a degradării sub pragul de 3 secunde impus de caiet.

Politicile SLA sunt date de business, administrabile din interfață, versionate, cu aprobare „patru ochi" la modificare. Catalogul inițial propus este în Anexa E din T3.

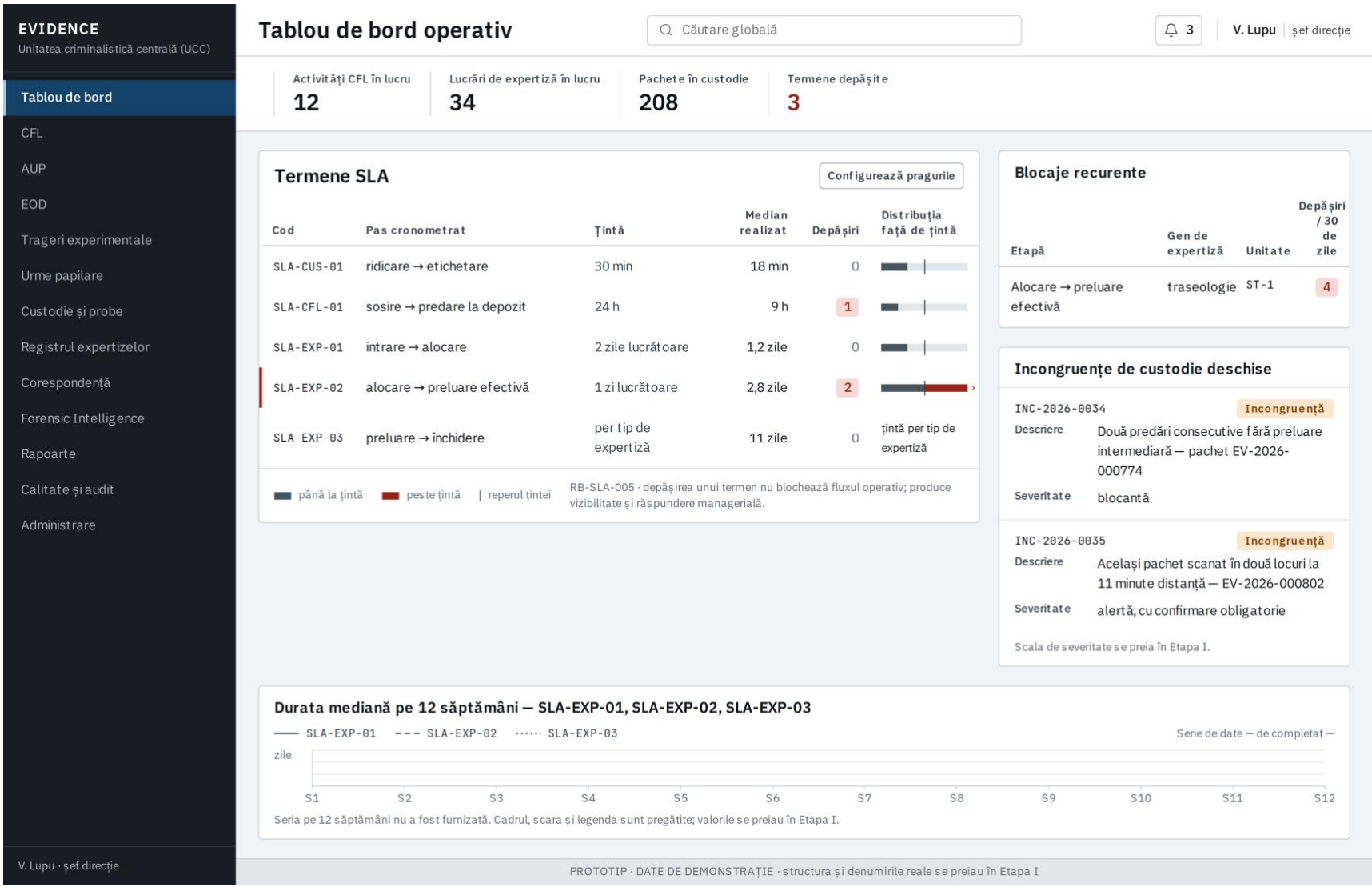


Figura 5. Tabloul de bord operativ. Fiecare politică SLA este un rând cu ținta, mediana realizată, numărul de depășiri și distribuția față de țintă; SLA-EXP-02 este singura peste țintă, la 2,8 zile față de o zi lucrătoare. Nota de subsol citează regula RB-SLA-005: depășirea unui termen nu blochează fluxul operativ, ci produce vizibilitate și răspundere managerială. În dreapta, incongruențele de custodie detectate automat. Panoul de jos păstrează cadrul graficului de tendință pe 12 săptămâni; seria se alimentează din datele reale ale beneficiarului, după migrare.

6.6 Semnătura electronică și principiul „patru ochi"

Modelul de semnare este agnostic față de furnizor. Sistemul definește *ce* se semnează (raportul de expertiză, planșa foto, procesul-verbal CFL, raportul EOD, documentele de corespondență, rapoartele oficiale), *cine* semnează și *în ce ordine*. Furnizorul efectiv — MSign sau mecanismul intern de asumare — este o implementare comutabilă. Consecința practică: dacă accesul la MSign întârzie din motive administrative, fluxurile funcționează în varianta internă și se comută ulterior, fără modificarea logicii.

„Patru ochi" se implementează în două straturi independente:

1. **În baza de date** — constrângere CHECK care interzice ca aprobatorul să fie identic cu inițiatorul, plus UNIQUE pe (subiect, pas, aprobator) care interzice aceeași persoană de două ori pe același pas. Regula devine imposibil de încălcat, nu doar verificată.
2. **În fluxul de semnare** — co-semnarea documentului, cu marcă temporală pentru fiecare semnatar.

Principiul se aplică nu doar livrabilelor operative, ci și modificărilor de configurație care afectează integritatea sistemului: politicile SLA, matricea de drepturi, nomenclatoarele operative.

6.7 Jurnalul de audit inviolabil

Caietul cere „urme de audit criptate și nealterabile pentru fiecare acces, modificare, validare, semnare, export sau sincronizare, cu utilizator, operațiune, dată/oră, durată, rezultat și IP sursă" [CS §6.2, p. 41 și §6.5, p. 41].

Soluția menține două jurnale distincte, cu roluri diferite:

Jurnal	Rol	Proprietăți
Operațional	Diagnostic tehnic, istoric per câmp, depanare	Tabele obișnuite, retenție configurabilă
Probatoriu	Valoare juridică, prezentabil în instanță	Append-only garantat la nivel de bază de date; lanț criptografic; sigilii temporale

Jurnalul probatoriu: privilegiile de actualizare, ștergere și trunchiere sunt revocate de la toate rolurile aplicației, plus un declanșator care blochează operațiunile inclusiv pentru proprietarul schemei. Fiecare înregistrare conține utilizatorul, rolul, IP-ul, sesiunea, acțiunea, tipul și identificatorul entității, starea fluxului, valorile vechi și noi, durata, rezultatul, amprenta înregistrării anterioare și amprenta proprie.

Amprenta se calculează cu cheie criptografică păstrată în afara bazei de date — în seiful de chei sau în modulul hardware al beneficiarului. Aceasta este diferența dintre un lanț decorativ și unul apărabil: un administrator de bază de date cu acces total nu poate recalcula lanțul fără cheie, deci nu poate rescrie istoria fără ca modificarea să devină detectabilă.

Periodic, un proces emite un sigiliu — rezumatul intervalului, semnat cu marcă temporală calificată, stocat separat. Un punct de verificare reparcurge lanțul și raportează prima poziție unde amprenta nu se potrivește. Acesta este artefactul care se prezintă în instanță și în raportul de audit.

Paralel, evenimentele cu relevanță juridică se trimit în MLog, iar jurnalul se replică append-only pe infrastructură administrată separat, pentru detectarea divergențelor.

Alertele automate de integritate cerute de caiet — tentative de ștergere, autentificări multiple, acces neautorizat — se completează cu detecția de anomalii de comportament: acces în afara orelor de program, volum anormal de export, accesări repetate ale aceluiași dosar de către un utilizator neimplicat în el. Un sistem cu date criminalistice este o țintă de exfiltrare, iar cerința de „alerte la anomalii" exact aceasta o vizează.

Ce înseamnă „nealterabil", operațional. Cerința caietului este îndeplinită în sensul cel mai puternic care se poate demonstra tehnic și susține juridic: orice modificare a jurnalului devine detectabilă și localizabilă la poziția exactă, inclusiv o modificare efectuată de un administrator cu acces total la baza de date. Punctul de verificare a lanțului produce, la cerere, raportul care atestă integritatea intervalului sau indică prima poziție compromisă. Acesta este artefactul care se prezintă în instanță și în raportul de audit — și este mai puternic decât o declarație de inviolabilitate, tocmai pentru că este verificabil de un terț.

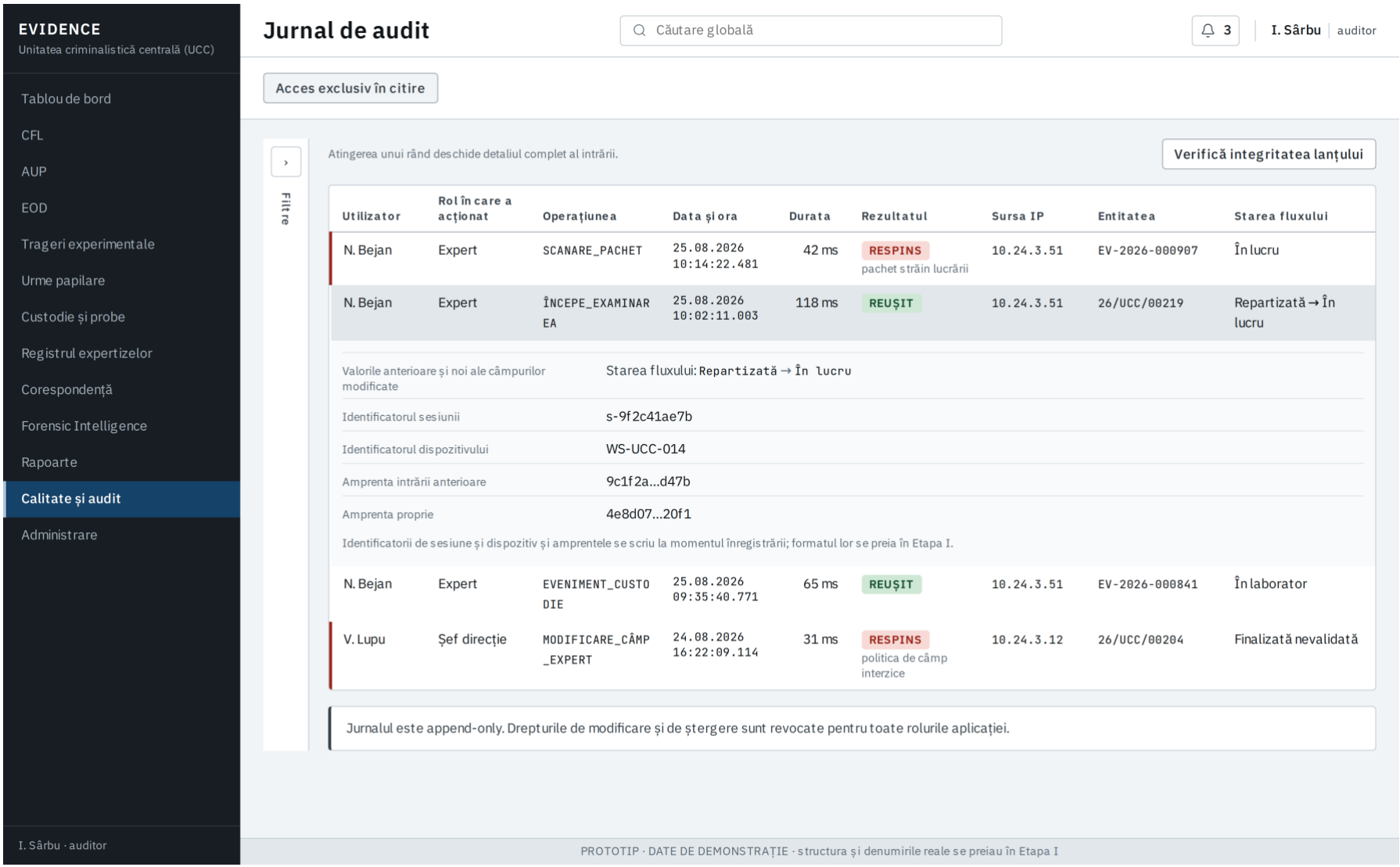


Figura 6. Jurnalul de audit probatoriu, în rolul de auditor — acces exclusiv în citire. Fiecare intrare poartă utilizatorul, rolul în care a acționat, operațiunea, momentul la milisecundă, durata, rezultatul, IP-ul sursă, entitatea și starea fluxului. Rândul deschis arată valorile vechi și noi, identificatorii de sesiune și dispozitiv și cele două amprente care formează lanțul de integritate. Ultimul rând este dovada mecanismului din §8.2: o tentativă a șefului de direcție de a modifica un câmp introdus de expert, respinsă cu motivul politica de câmp interzice.

6.8 Lucrul offline și reconcilierea

Aplicația de teren este o PWA separată, nu o rută în back-office. Motivul: pachet mic, service worker agresiv, model de date local, ciclu de livrare propriu, optimizare pentru tabletă.

Local: shell-ul și resursele în cache gestionat, datele structurate în IndexedDB, fotografiile în sistemul de fișiere privat al originii. Fiecare acțiune produce un eveniment într-un outbox, cu identificator unic generat pe client — idempotența este garantată de server pe această cheie, deci retransmiterea nu produce duplicate.

Sincronizare: un punct de trimitere care returnează, per eveniment, „aplicat" sau „conflict", și un punct de descărcare a modificărilor de la un cursor. Descărcarea este filtrată strict pe subunitate, rol și cazuri atribuite. Nu se descarcă niciodată setul complet de date pe dispozitiv — într-un sistem de poliție, un dispozitiv pierdut nu trebuie să conțină decât cazurile utilizatorului său.

Semantica conflictelor, în două grade:

- *actualizare paralelă* — versiuni diferite, proprietăți diferite → severitate mică, se aplică automat și se marchează;
- *conflict propriu-zis* — aceleași proprietăți modificate în ambele părți → nu se aplică automat, intră într-un ecran dedicat de reconciliere, cu decizie umană explicită și jurnalizare în auditul probatoriu.

Fotografiile se amprentează criptografic pe dispozitiv, la captură, înainte de orice transfer. Acesta este argumentul tehnic că fișierul nu s-a modificat între teren și server, independent de semnătura aplicată ulterior.

Acesta este cel mai mare bloc de risc tehnic al proiectului și este tratat ca atare în planificare: nucleul de sincronizare începe în Etapa II, în paralel cu arhitectura, nu în Etapa III împreună cu restul dezvoltării. Testarea pe conectivitate degradată este activitate distinctă în planul de testare.

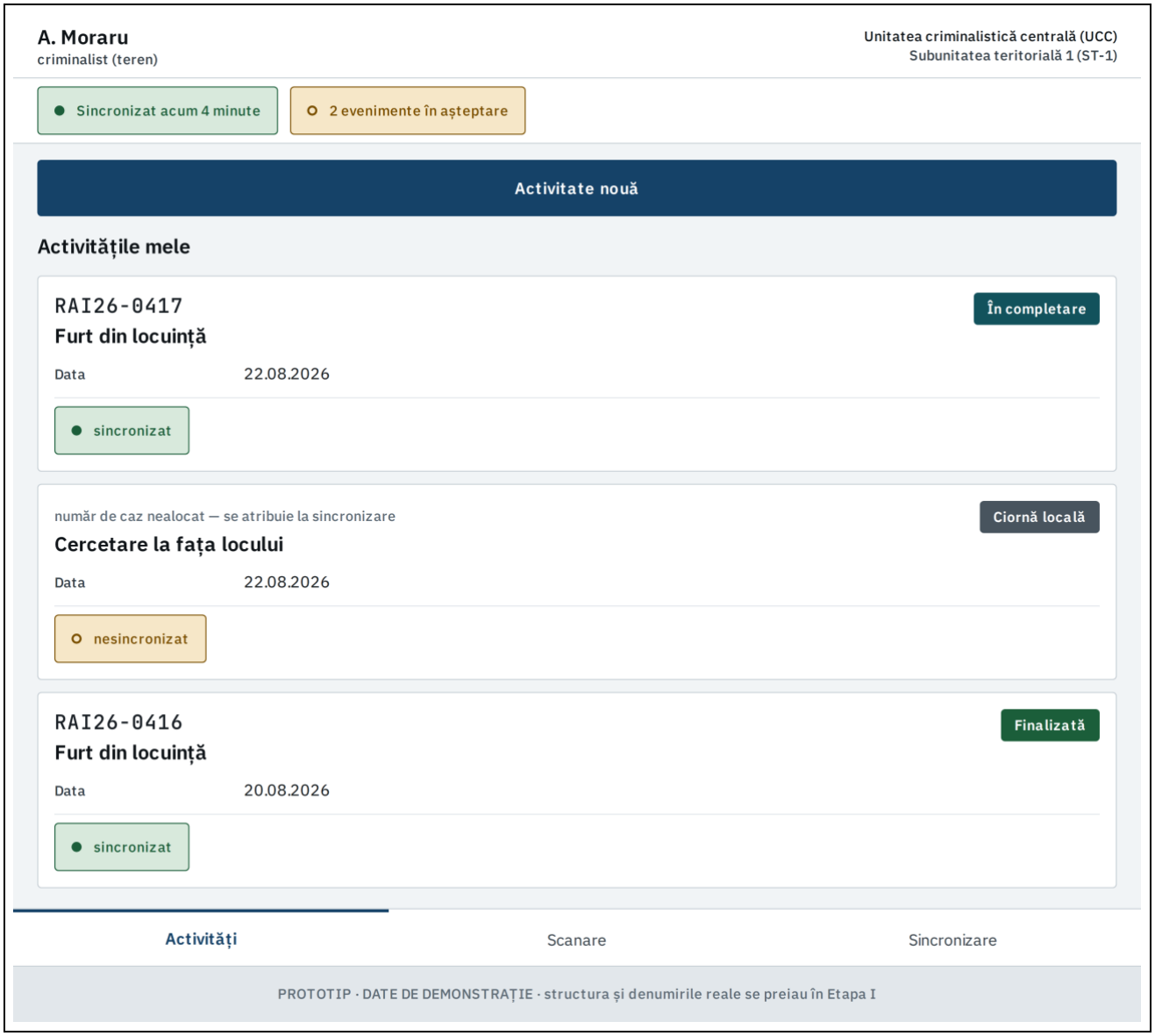


Figura 7. Aplicația de teren, lista activităților criminalistului. Fiecare activitate poartă starea de sincronizare, iar o activitate creată offline apare ca „Ciornă locală", cu mențiunea că numărul de caz nu este încă alocat: identificatorul se atribuie de server la sincronizare, pentru a nu produce numere duplicate între dispozitive.

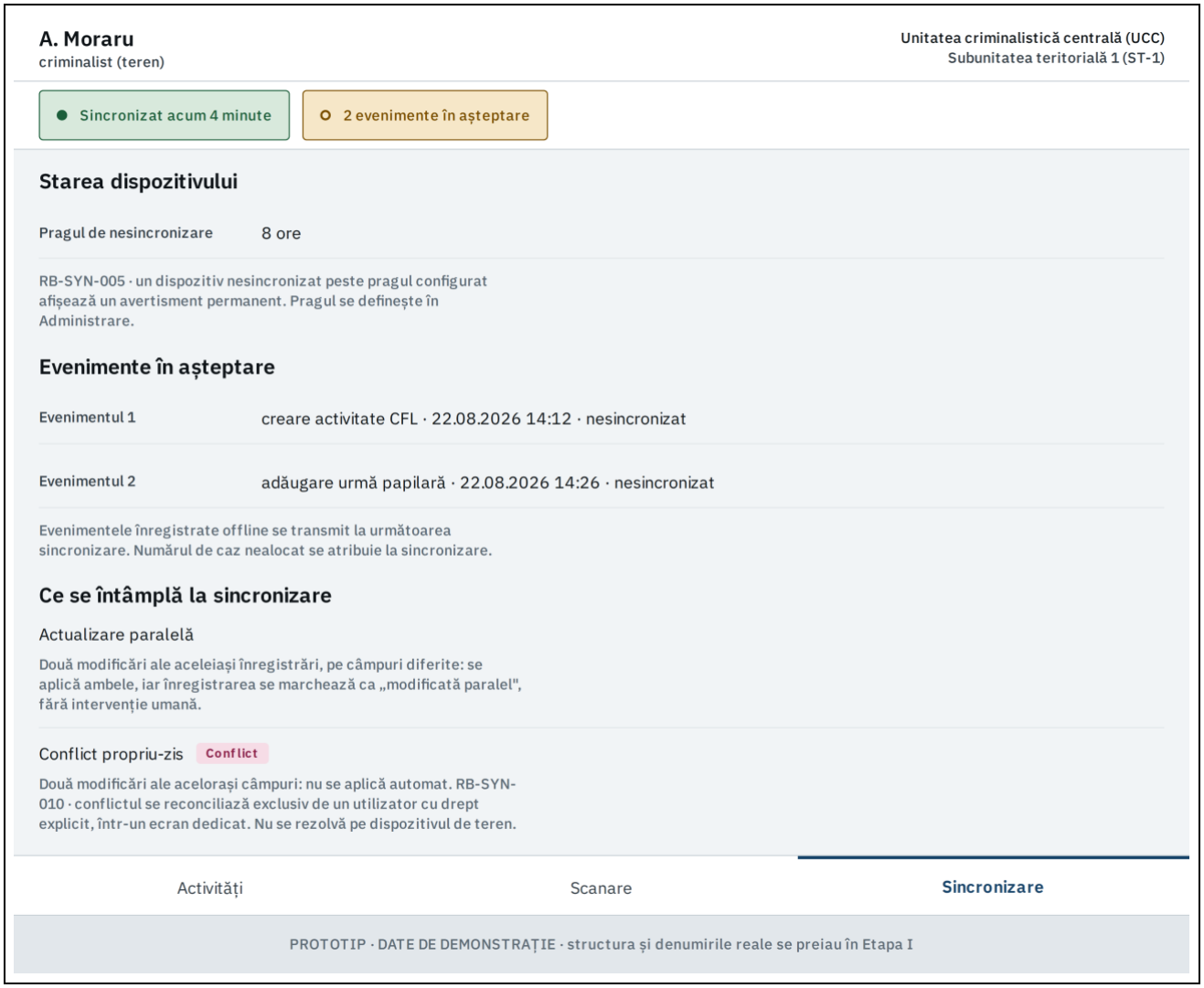


Figura 8. Starea dispozitivului și semantica de conflict, în aplicația de teren. Evenimentele înregistrate offline stau într-un outbox până la următoarea sincronizare. Cele două grade de conflict sunt explicate direct în interfață: actualizarea paralelă se aplică automat și se marchează, în timp ce conflictul propriu-zis nu se aplică și se reconciliază exclusiv într-un ecran dedicat, de către un utilizator cu drept explicit — niciodată pe dispozitivul de teren.

6.9 Căutare, filtrare și vizibilitate

Comportamentul existent se păstrează: căutarea pe interval prin suprapunere, filtrele pe unitate și subunitate, ascunderea entităților dezactivate din listele operative, dependența listei de străzi de localitatea selectată.

Extindere: căutarea inter-modulară cerută de M9 și M11 — o persoană, un obiect, un număr de caz sau un cod de bare se caută o singură dată și returnează rezultate din toate modulele la care utilizatorul are drept de acces. Rezultatele sunt filtrate prin același mecanism de vizibilitate ca ecranele operative: căutarea nu poate deveni o portiță prin care un utilizator vede ce nu ar vedea în modulul respectiv. Fiecare căutare se jurnalizează.

6.10 Nomenclatoare, versionare și ferestre de valabilitate

M14 cere un registru centralizat de taxonomii cu versionare și ferestre de valabilitate. Aceasta nu este o funcționalitate în plus, ci o schimbare de model: astăzi, redenumirea unei unități rescrie retroactiv toate rapoartele istorice. Cu ferestre de valabilitate, fiecare înregistrare păstrează referința la versiunea nomenclatorului valabilă la momentul faptei, iar rapoartele istorice rămân corecte.

Toate nomenclatoarele operative — unități, funcții, grade, autoturisme, localități, străzi, fapte, moduri de operare, locuri de comitere, intervale de lucru, zile libere, taxonomii EOD, genuri și specialități de expertiză

— trec sub acest model. Modificările sunt supuse aprobării „patru ochi" și se jurnalizează în auditul probatoriu.

7. Interoperabilitatea

7.1 Principiul de izolare

Un singur modul — M10 — comunică cu exteriorul. Fiecare conector implementează aceeași interfață, produce aceleași evenimente de audit și respectă același contract de tratare a erorilor. Restul sistemului nu știe dacă un identificator extern a fost introdus manual sau preluat prin API.

Consecința: activarea unui conector nou nu modifică logica modulelor operative, iar indisponibilitatea unui sistem extern nu blochează activitatea internă.

7.2 Platformele guvernamentale (HG nr. 822/2020)

Platformă	Utilizare	Statut
MPass	Autentificare federată, cu provisioning pe IDNP	Opțional, comutabil din configurație [CS §6.2]
MSign	Semnare cu marcă temporală calificată, co-semnare	Opțional, cu alternativă internă [CS §6.2]
MConnect	Preluarea datelor din registrele de stat, conform principiului *once-only*; adrese și străzi din registrul de adrese	Propus
MConnect Events	Publicarea evenimentelor de domeniu relevante, în format CloudEvents	Propus — satisface cerința AGE de arhitectură event-driven
MNotify	Notificări multicanal la depășirea termenelor și la evenimente critice	Propus
MLog	Jurnalizarea evenimentelor cu relevanță juridică	Propus
MCloud	Găzduirea soluției, sub administrarea tehnică STISC	Conform principiilor AGE

Formalitățile administrative de conectare — Formularul Unic de Conectare la AGE, certificatul de sistem de la STISC, accesul la mediile de testare — se depun în prima săptămână a Etapei I. Termenul declarat este de maximum 7 zile lucrătoare de la dosarul complet, gratuit pentru instituțiile publice, dar într-un contract care se încheie la 31 decembrie 2026 nu există marjă pentru întârzieri. Arhitectura cu comutare (§2.2) este mecanismul care asigură că o întârziere administrativă nu blochează livrarea.

7.3 Sistemele criminalistice externe

Modelul în două trepte, exact cum îl permite caietul:

Treapta 1 — implicit, inclus în preț. Identificatorul extern este atribut de primă clasă al entității: validare de format, verificare de unicitate, jurnalizarea fiecărei modificări, căutare și raportare pe el. Funcționează cu introducere manuală, independent de orice API.

Treapta 2 — condiționat. Conector REST/JSON sau SOAP cu autentificare mutuală pe bază de certificate digitale, mapare documentată câmp-la-câmp, evenimente de creare/actualizare/ștergere, tratarea erorilor și a neconcordanțelor de versiune, reconciliere programată și arhivarea completă a schimburilor în jurnalul inviolabil.

Pentru AFIS, oferta include un element pe care ofertantul îl consideră diferențiator: un serviciu intern de împachetare care construiește tranzacții în formatul standard ANSI/NIST-ITL 1-2011 (înregistrări de tip 1, 2, 9, 13, 14), cu codarea imaginilor în formatul de compresie standard pentru amprente. Sistemul produce astfel pachete conforme standardului internațional indiferent dacă un conector este activ sau nu — ceea ce

înseamnă că, în momentul în care AFIS expune o interfață, integrarea se reduce la transport, nu la conversie de format.

Pentru balistică, oferta livrează integral ceea ce solicită caietul: registrul, caracteristicile tehnice ale armelor, loturile de tragere, identificatorii externi EVOFINDER și TRAFFIC și arhitectura conectorului. Compararea balistică propriu-zisă rămâne, ca și astăzi, în sarcina sistemelor specializate ale beneficiarului — sisteme proprietare, cu hardware dedicat de scanare 3D, pe care caietul nu cere să fie înlocuite. EVIDENCE le referențiază și se integrează cu ele, nu le duplică.

7.4 Tipărirea etichetelor în teren — precizare tehnică

Caietul cere tipărirea etichetelor cu coduri de bare pe imprimante mobile, din aplicația de teren, și, separat, funcționarea pe Chrome, Edge și Firefox.

Comunicarea directă a unei aplicații web cu o imprimantă Bluetooth se face prin Web Bluetooth, interfață implementată în Chrome și Edge, dar nu în Firefox. Aceasta este o limitare a browserului, nu a soluției.

Cerința este îndeplinită pe toate cele trei browsere. Aplicația EVIDENCE rulează integral din browser, fără instalare locală, pe Chrome, Edge și Firefox. Comunicarea cu o imprimantă Bluetooth este însă o funcție de periferic, nu o funcție a aplicației web, iar ofertantul o livrează în două forme complementare, ambele incluse în preț:

1. **Tipărire directă din browser**, pe Chrome și Edge, fără nicio componentă suplimentară — varianta recomandată pe dispozitivele de teren, pentru simplitate operațională.
2. **Driver companion Android open source**, dezvoltat și livrat de ofertant, care mediază comunicarea cu imprimanta pentru orice browser, inclusiv Firefox. Componenta este un utilitar de periferic, comparabil cu driverul unei imprimante de birou; aplicația EVIDENCE rămâne integral web, fără instalare.

Beneficiarul alege în Etapa I care variantă se desfășoară pe fiecare categorie de dispozitiv. Ambele sunt dezvoltate, testate și predate.

8. Securitatea

8.1 Conformitatea cu cerințele din caiet

Cerință [CS §6.2, p. 40–41; §6.5, p. 41]	**Soluția ofertată**
Conformitate ISO/IEC 27001, 27002, 27005	Controalele aplicabile sunt implementate în proiectare, dezvoltare și operare. Livrabilul de politici de securitate (Caietul de sarcini, cap. 8.1, pct. 7) include o matrice control ISO → mecanism implementat → dovadă, care permite beneficiarului să verifice conformitatea control cu control
Criptare **AES-256**	Criptare la repaus la nivel de volum sau bază de date, plus criptare la nivel de câmp pentru datele sensibile, cu chei gestionate în seif și rotație documentată
RBAC/ABAC cu granularitate pe rol și atribut	Trei niveluri: permisiuni de acțiune, filtre de vizibilitate pe înregistrări, matrice câmp × stare (§8.2)
Administrare locală a utilizatorilor cu politici configurabile	Complexitate, expirare, blocare la încercări repetate, istoric de parole — toate configurabile
MPass opțional pentru SSO și MFA	MFA prin cod temporal funcționează independent de MPass
Semnare prin MSign **sau mecanisme interne**	Ambele, comutabile (§6.6)
Audit criptat și nealterabil	§6.7
Alerte automate de integritate și rapoarte periodice către administratorul de securitate	§6.7, plus detecția de anomalii comportamentale

8.2 Autorizarea pe trei niveluri

Cerința „RBAC/ABAC cu granularitate pe câmp, acțiune și stare" este, în opinia ofertantului, cerința cea mai des tratată superficial în ofertele pentru sisteme de acest tip. Ea se descompune în trei întrebări diferite, care cer trei mecanisme diferite:

Întrebarea	Mecanismul	Exemplu
Ce acțiuni are voie rolul?	Permisiuni ierarhice, verificate la intrarea în fiecare serviciu de aplicație	Șeful de direcție are permisiunea de repartizare; expertul nu
Ce înregistrări vede?	Filtre de date aplicate automat la nivelul stratului de acces, nu în fiecare interogare	Criminalistul vede doar propriile activități CFL; șeful de secție vede subunitatea; auditorul vede tot, dar numai în citire
Ce câmp are voie să atingă, în ce stare a fluxului?	Matricea FieldPolicy(rol, entitate, stare, câmp, acces), evaluată la fiecare citire și la fiecare scriere	După validare, expertul nu mai poate modifica niciun câmp al rezultatului; secretariatul poate opera exclusiv câmpurile de expediere; șeful de direcție nu poate modifica niciun câmp introdus de expert, în nicio stare

Al treilea nivel este cel care implementează regula centrală a sistemului actual — *niciun rol nu poate modifica datele introduse de alt nivel*. Fără el, regula rămâne o convenție de interfață, ocolibilă prin API.

La citire, câmpurile interzise se elimină din răspuns înainte de serializare — nu se ascund în interfață. La scriere, o modificare neautorizată se respinge cu cod de eroare și cu numele câmpului respins, pentru ca utilizatorul să înțeleagă ce s-a întâmplat. Matricea se administrează din interfață, este versionată și supusă aprobării „patru ochi".

Efectul mecanismului este vizibil în prototip: jurnalul de audit din §6.7 conține o tentativă de modificare respinsă cu motivul politica de câmp interzice, produsă de un utilizator cu rol de șef de direcție asupra unui câmp introdus de expert.

Matricea completă rol × entitate × stare × câmp, pentru entitățile principale, este în Anexa D din T3. Ea este simultan specificația de implementare și planul de testare al acestui mecanism: fiecare celulă este un caz de test.

8.3 Securitatea în ciclul de dezvoltare

Secretele nu apar niciodată în cod sau în imaginile de container: se injectează la execuție din seiful de chei. Containerele rulează fără privilegii de root, cu sistem de fișiere în citire, cu politici de rețea restrictive.

În integrarea continuă rulează automat: analiză statică de cod, scanarea dependențelor pentru vulnerabilități cunoscute, scanarea imaginilor de container, generarea automată a inventarului de componente software (SBOM). Acest din urmă artefact servește direct ca dovadă de conformitate de licențiere pentru Anexa T2 și se actualizează la fiecare livrare — deci afirmația „fără costuri de licențe" rămâne verificabilă pe toată durata contractului, nu doar la ofertare.

Limitarea de debit și protecția anti-automatizare se aplică pe punctele de căutare și export.

8.4 Datele cu caracter personal

Sistemul procesează date cu caracter personal din categorii speciale: date privind faptele penale, date biometrice (urme papilare), date de localizare. Proiectarea aplică principiile de protecție a datelor prin concepție:

– **minimizarea** — descărcarea pe dispozitivele de teren este filtrată pe cazurile atribuite, nu integrală;
– **limitarea scopului** — accesul se acordă pe implicarea în caz, nu pe apartenența la instituție;

– **trasabilitatea** — fiecare acces la o înregistrare cu date personale se jurnalizează, inclusiv simpla consultare;
– **retenția** — politici de arhivare și de ștergere configurabile pe categorie de date.

> **Punct de clarificat în Etapa I.** Caietul de sarcini invocă „Legea nr. 506/2004", act normativ din România, nu din Republica Moldova, unde se aplică Legea nr. 133/2011 privind protecția datelor cu caracter personal (citată corect în anunțul de participare). Textul caietului menționează și „realitatea administrativă a României" în descrierea structurilor geografice. Ofertantul a proiectat pe cadrul normativ al Republicii Moldova și solicită confirmarea în Etapa I.

9. Performanța, disponibilitatea și continuitatea operațională

9.1 Parametrii impuși și mecanismele care îi susțin

Parametru [CS §6.3, p. 41; §6.6, p. 42]	Valoare impusă	Cum se atinge	Cum se demonstrează
Timp de răspuns	sub 3 s pentru 95% din interogările uzuale	Separarea raportării de datele operative; indexare țintită; indecși parțiali pe cozile de lucru; cache pentru nomenclatoare; paginare obligatorie	Teste de încărcare automate, rulate în integrarea continuă pe scenariile reale de utilizare; raport la fiecare recepție parțială
Disponibilitate	minimum 99,5% în intervalele de lucru instituțional	Replici multiple ale serviciului API în spatele unui echilibrator; bază de date în configurație de înaltă disponibilitate cu replicare sincronă; failover automat	Monitorizare continuă cu obiective de nivel de serviciu urmărite explicit; raport lunar. *Intervalele de lucru instituțional se definesc în scris în Etapa I și se anexează la contract, astfel încât indicatorul să fie măsurabil identic de ambele părți.*
Pierdere maximă de date acceptată (RPO)	nespecificată în caiet	Replicare sincronă a bazei de date și arhivarea continuă a jurnalului de tranzacții permit un RPO sub 5 minute pentru datele din back-office. Pentru datele create offline, RPO-ul este determinat de momentul ultimei sincronizări a dispozitivului	Exercițiu de restaurare la un moment în timp, cu măsurarea pierderii efective
Backup	zilnic, criptat, în locații distincte, minimum 7 versiuni	Backup criptat automat, în două locații, plus arhivarea continuă a jurnalului de tranzacții pentru restaurare la un moment în timp	Testare automată lunară a restaurării, cu raport
Restaurare completă (RTO)	maximum 6 ore	Procedură documentată și repetată	Exercițiu de restaurare efectuat și cronometrat, cel puțin o dată înainte de recepția finală
Optimizări BD	indexare, particionare, arhivare automată a datelor istorice	Particionarea tabelelor cu creștere rapidă (evenimente de custodie, jurnal de audit) pe interval temporal; arhivare automată configurabilă	Plan de întreținere documentat
Reziliență	cache, gestionarea conexiunilor, limitarea resurselor, failover, replicare	Toate implementate la nivel de infrastructură și aplicație	Testare de reziliență în Etapa III

> **Observație de metodă.** Un obiectiv de restaurare în 6 ore rămâne o afirmație atâta timp cât restaurarea nu se testează periodic. De aceea testarea automată lunară a restaurării din backup este inclusă ca procedură operațională standard, cu raport, nu ca activitate opțională.

9.2 Planul de continuitate

Se livrează, conform cerinței, un plan de continuitate operațională și proceduri de recuperare în caz de dezastru, care acoperă: pierderea unui nod de aplicație, pierderea instanței principale de bază de date, coruperea datelor, indisponibilitatea unui serviciu extern, pierderea unui dispozitiv de teren cu date locale nesincronizate.

Ultimul scenariu merită menționat explicit: dispozitivele de teren conțin date operative nesincronizate. Procedura acoperă ștergerea de la distanță, invalidarea sesiunii și reconstituirea evenimentelor pierdute din jurnalul serverului.

10. Migrarea din sistemul actual

10.1 De ce are tratament propriu

Caietul de sarcini nu conține un capitol de migrare. Prin clarificarea din 5 august, autoritatea confirmă însă că prestatorul primește structura bazei de date și datele existente, iar sistemul actual este în exploatare cu utilizatori activi.

Un proiect care rescrie un sistem în producție fără un plan de migrare nu se poate finaliza. Ofertantul îl include în ofertă din proprie inițiativă și l-a ridicat ca solicitare de clarificare.

10.2 Abordarea propusă

Un proiect de migrare distinct, cu mapare declarativă vechi → nou, rulare repetabilă și idempotentă — se poate executa de câte ori este nevoie, cu același rezultat — și raport de reconciliere pe fiecare tabel: rânduri în sursă, rânduri migrate, rânduri respinse, cu motivul respingerii. Nicio migrare nu se consideră reușită pe baza absenței erorilor; se consideră reușită pe baza raportului de reconciliere acceptat de beneficiar.

Analiza migrării intră în Etapa I, execuția în Etapa V. Ofertantul propune o fereastră de rulare în paralel a celor două versiuni în unitatea-pilot, ca măsură de reducere a riscului; durata și modul de operare se stabilesc de comun acord în Etapa I, în funcție de capacitatea operativă a beneficiarului.

10.3 Zonele de atenție

Zonă	Problemă anticipată	Tratament
Identificatorii istorici	ID-urile de caz CFL și numerele de expertiză existente trebuie păstrate exact, iar generarea numerelor noi trebuie să continue de la valorile actuale	Secvențele se inițializează din datele migrate; nu se renumerotează nimic
Codurile de bare emise	Un cod emis în sistemul vechi nu poate fi realocat în cel nou	Codurile migrate se marchează ca folosite, indiferent de starea pachetului
Nomenclatoarele fără ferestre de valabilitate	Sistemul actual nu păstrează versiuni istorice ale denumirilor	Valorile actuale se importă cu fereastră deschisă retroactiv; se documentează că rapoartele anterioare migrării folosesc denumirile curente
Datele incomplete	Un sistem în exploatare de patru ani conține înregistrări care nu respectă constrângerile noi	Se migrează într-o zonă de carantină, cu raport pentru decizia beneficiarului — nu se șterg și nu se completează automat

Zonă	Problemă anticipată	Tratament
Lanțul de custodie al pachetelor migrate	Pachetele existente nu au istoric complet de mișcări în noul model	Fiecare pachet migrat primește un eveniment de custodie inițial, marcat explicit „preluat din sistemul precedent", cu data migrării și custodele declarat. Lanțul nou pornește de la un punct cunoscut, nu de la o discontinuitate
Conturile de utilizator	Parolele din sistemul vechi nu se pot și nu trebuie preluate	Conturile se migrează cu identitatea, rolurile și dosarul de personal; parolele **nu** se migrează. La prima autentificare, utilizatorul își stabilește o parolă conformă cu noile politici sau se autentifică prin MPass
Continuitatea codurilor de bare	Codurile emise de sistemul nou nu trebuie să se suprapună peste cele istorice	Generatorul de coduri se inițializează pe un **interval disjunct** față de codurile migrate; suprapunerea devine imposibilă prin construcție, nu prin verificare
Jurnalul de audit istoric	Auditul vechi nu are lanț criptografic	Se importă ca istoric, marcat explicit ca „preluat, fără lanț de integritate". Lanțul începe de la data punerii în funcțiune a sistemului nou. Alternativa — a pretinde integritate criptografică pentru date care nu o au — ar compromite credibilitatea întregului mecanism

Partea III — Realizarea

11. Metodologia de implementare

11.1 Agile cu milestone-uri cu poartă

Caietul impune metodologia: *Agile with gated milestones* [CS §7.1, p. 42] — iterații scurte în interiorul fiecărei etape, dar fiecare etapă închisă printr-o recepție parțială documentată și un raport de validare.

Ofertantul o aplică astfel:

În interiorul etapei — iterații de două săptămâni, fiecare încheiată cu o versiune funcțională desfășurată în mediul de testare al beneficiarului și cu o demonstrație. Beneficiarul vede sistemul crescând, nu doar rapoarte de progres. Modificările de detaliu se pot absorbi în iterația următoare, fără renegociere.

La granița dintre etape — o poartă formală: livrabilele etapei se predau, se verifică față de criterii stabilite înainte de începerea etapei, iar recepția parțială se semnează. Fără semnătură pe poarta anterioară, etapa următoare nu începe formal.

Combinația este esențială într-un contract cu termen fix și scop parțial nespecificat: iterațiile absorb detaliile, porțile protejează amploarea.

11.2 Definiția de „terminat"

Pentru a evita disputele la recepție, ofertantul propune, ca element de aprobat în Etapa I, o definiție unică de „terminat" aplicabilă fiecărei unități de lucru:

O funcționalitate este terminată când: codul este scris și revizuit de o a doua persoană („patru ochi" pe fiecare livrabil, conform cap. 7.3); testele automate care acoperă regulile ei trec; criteriile de acceptanță CA-* corespunzătoare din Anexa T3 sunt verificate; documentația de utilizare a ecranelor afectate este actualizată; funcționalitatea este desfășurată în mediul de testare al beneficiarului.

Definiția este verificabilă și se aplică uniform. Ea transformă „gata în proporție de 80%" — cea mai costisitoare formulare dintr-un proiect cu termen fix — într-o afirmație care nu se mai poate face.

11.3 Ordinea de implementare

Ordinea nu este cea din numerotarea modulelor din caiet, ci cea impusă de dependențe și de risc:

Rang	Ce se construiește	De ce în această ordine
1	Administrare și Identitate	Fundația întregului sistem: nomenclatoare, unități, utilizatori, drepturi. Fără ea, niciun alt modul nu poate defini cine ce vede.
2	Custodie	Fundația probatorie. Fără lanțul de custodie, nici CFL, nici Expertizele nu se pot închide corect.
3	CFL și Registrul expertizelor, în paralel	Cele mai mari module și, totodată, singurele specificate în detaliu în caiet. Se construiesc pe fundația deja existentă.
4	AUP, EOD, Balistică, Dactiloscopie, Corespondență	Module operative, fiecare pe aceeași fundație de custodie și identitate.
5	Interoperabilitate, Rapoarte, Intelligence, Calitate	Straturi care consumă datele produse de celelalte module; ordinea le plasează în urma surselor lor.

În paralel cu toate, din Etapa II: nucleul de sincronizare offline, mecanismul de autorizare pe câmp × stare și jurnalul de audit probatoriu. Împreună cu lanțul de custodie (§6.4), acestea sunt cele patru cerințe fără soluție de raft identificate în §1.4; ele nu se pot lăsa la final, pentru că restul sistemului se construiește peste ele.

Raționamentul ordinii: dacă proiectul ar întâmpina dificultăți, ceea ce trebuie să existe și să funcționeze impecabil este lanțul CFL → custodie → expertiză → raport semnat, cu audit și drepturi corecte. Este fluxul care produce documente cu valoare juridică. Un modul de analiză livrat parțial este o pierdere; un lanț de custodie livrat parțial este un sistem inutilizabil.

12. Etapele, livrabilele și criteriile de recepție

Cele șase etape din cap. 7.2 al Caietului de sarcini, în intervalul 27 august – 31 decembrie 2026, cu suprapuneri planificate.

Etapa I — Analiza cerințelor și modelarea de business

Durată: 3 săptămâni · Suprapunere: ultima săptămână cu Etapa II

Activitate	Rezultat
Interviuri și workshopuri cu structurile operative	Procese-verbale, lista de decizii, lista de puncte deschise
Analiza codului sursă, a schemei de bază de date și a datelor primite	Model AS-IS complet — din caiet **și** din sistemul real
Analiza disfuncțiilor sistemului actual	Registrul disfuncțiilor, cu propuneri de tratare
Formalizarea modelului TO-BE, pornind de la Anexa T3	Model TO-BE aprobat formal
Dicționarul de date	Entități, atribute, tipuri, constrângeri
Diagrame BPMN pentru fluxurile principale	Diagrame aprobate
Planul de integrare inter-sistem	Inventarul integrărilor, cu statut și dependențe
Analiza migrării datelor	Plan de migrare, cu mapare și strategie de reconciliere
Depunerea dosarelor administrative la AGE și STISC	Formular Unic de Conectare, cerere de certificat de sistem, cerere de acces la mediile de testare

Criteriul de poartă: modelul TO-BE, dicționarul de date și diagramele BPMN sunt aprobate formal de beneficiar și devin bază de referință contractuală. Orice cerință care apare ulterior și nu se regăsește în model se tratează prin procedura de control al modificărilor.

Este cel mai important element contractual al proiectului, dat fiind că cele 14 module ocupă patru pagini în caiet. El protejează beneficiarul (primește exact ce a descris, verificabil) și prestatorul (scopul devine finit).

Etapa II — Arhitectura software și designul detaliat

Durată: 3 săptămâni · Suprapunere: parțială cu Etapele I și III

Activitate	Rezultat
Documentul de arhitectură și deciziile de arhitectură (ADR)	Arhitectura aprobată, **inclusiv componentele stack-ului convenite cu beneficiarul** (§4.2); ADR-uri pentru platformă și SGBD, identitate, workflow, stocare, cache distribuit, offline, model de nomenclatoare
Scheletul soluției, migrările de bază, integrarea continuă	Mediu de dezvoltare și de testare funcțional

Activitate	Rezultat
Autentificarea end-to-end pe mediul de testare	Autentificare locală cu MFA, funcțională și demonstrată. Autentificarea prin MPass, demonstrată pe mediul de testare guvernamental dacă accesul a fost acordat până la acea dată
Prototipurile UI/UX pentru ecranele critice	Prototipuri aprobate de beneficiar [CS §7.2, pct. 2]
Startul nucleului de sincronizare offline	Prototip funcțional de outbox, sincronizare și detecție de conflicte
Planul de testare	Strategia, mediile, datele de test, criteriile de ieșire

Fluxurile principale supuse aprobării beneficiarului, conform cap. 7.2, pct. 2: cercetarea la fața locului, custodia și mișcarea probelor, registrul expertizelor, tragerile experimentale și marcarea armelor, ciclul urmelor papilare și schimbul cu AFIS, corespondența și rapoartele.

Ecranele prototipate prioritar în interiorul acestor fluxuri, pentru că în ele se decide acceptanța: adăugarea unei activități CFL (zeci de câmpuri cu afișare condiționată), predarea-preluarea unui pachet cu scanare de cod, repartizarea expertizei, examinarea cu scanare de coduri, înregistrarea unui lot de tragere cu identificator extern, evaluarea calitativă a unei urme papilare și pregătirea tranzacției AFIS, ecranul de reconciliere a conflictelor offline, tabloul de bord SLA.

Interfața respectă sistemul de design guvernamental al AGE acolo unde este aplicabil.

Criteriul de poartă: arhitectura și prototipurile UI/UX aprobate; autentificarea demonstrată end-to-end în varianta care nu depinde de terți; prototipul de sincronizare offline demonstrat pe conectivitate întreruptă. Demonstrarea autentificării prin MPass intră în criteriul de poartă numai în măsura în care accesul la mediul de testare guvernamental a fost acordat până la acea dată.

Etapa III — Dezvoltarea, integrarea și testarea internă

Durată: 9 săptămâni · Suprapunere: primele săptămâni cu Etapa II, ultimele 3 săptămâni cu Etapa IV

Dezvoltarea în ordinea din §11.3, cu livrare incrementală în mediul de testare al beneficiarului la fiecare două săptămâni.

Testarea internă, conform cerinței [CS §7.2, pct. 3]:

Tip	Acoperire
Testare unitară	Regulile de domeniu, invarianții, mașina de stare
Testare de integrare	Migrările, constrângerile, procedurile stocate, filtrele de vizibilitate — rulate pe o bază de date reală, nu simulată
Testare de contract	Concordanța dintre frontend și backend, verificată automat față de specificația OpenAPI
Testare end-to-end	Fluxurile complete, pe fiecare rol
Testare de performanță	Pragurile de 3 s și 99,5% din caiet, pe volume realiste
Testare de securitate	Scanări automate în integrarea continuă; verificarea matricei de drepturi celulă cu celulă
Testare de interoperabilitate	Conectorii activi, pe mediile de testare guvernamentale
Testarea semnării	Ambele variante — externă și internă
Testare offline	Sincronizare, conflicte, reconciliere, pe rețea simulată degradată

Prioritatea de acoperire cu teste: mașina de stare, matricea câmp × stare, lanțul de custodie și lanțul de audit. Acestea sunt regulile pe care le verifică beneficiarul la UAT și pe care se contestă un raport de expertiză în instanță.

Criteriul de poartă: toate modulele livrate în mediul de testare; rapoartele de testare internă predate; criteriile de acceptanță CA-* acoperite cu teste automate în proporția convenită în Etapa I.

Etapa IV — Testarea de acceptanță la beneficiar (UAT)

Durată: 3 săptămâni · Suprapunere: cu Etapa III

UAT-ul se desfășoară pe module, pe măsură ce se închid, nu la final. Aceasta este singura variantă compatibilă cu un interval de patru luni: un UAT concentrat în ultimele trei săptămâni ar descoperi problemele când nu mai există timp pentru corectare.

Activitate	Rezultat
Sesiuni de testare cu utilizatori reali, pe scenarii construite din criteriile CA-*	Rapoarte de testare
Registrul neconformităților, cu clasificare pe severitate	Registru actualizat continuu, vizibil beneficiarului
Corectare iterativă	Versiuni corectate, cu retestare

Criteriul de poartă: zero neconformități critice și majore deschise; neconformitățile minore, cu plan de remediere agreat.

Etapa V — Pilotul și implementarea la nivel național

Durată: 3 săptămâni

Activitate	Rezultat
Desfășurarea în producție, pe MCloud	Mediu de producție funcțional
Execuția migrării datelor, cu raport de reconciliere	Raport acceptat de beneficiar
Pilot într-o unitate de referință, cu rulare în paralel a celor două versiuni	Raport de pilot
Instruirea utilizatorilor din unitatea-pilot	Sesiuni desfășurate, materiale predate
Extinderea la nivel național, pe valuri	Rollout finalizat
Instruirea celorlalte categorii de personal	Sesiuni desfășurate

Criteriul de poartă: raportul de migrare acceptat; pilotul încheiat fără incidente critice; sistemul în exploatare la toate unitățile.

Etapa VI — Suportul post-implementare și transferul de cunoștințe

Durată: 12 luni de la punerea în funcțiune

Obligație [CS §8.3, p. 44]	Angajamentul ofertantului
Remedierea incidentelor critice	maximum **24 de ore**
Remedierea incidentelor minore	maximum **5 zile lucrătoare**
Actualizări periodice de securitate	Lunar, plus imediat la vulnerabilități critice publicate
Asistență online și telefonică	În intervalul de lucru al beneficiarului
Canal securizat de ticketing	Sistem dedicat, cu conturi pentru echipa beneficiarului
Transfer complet de cunoștințe	Documentație, sesiuni tehnice cu personalul IT al beneficiarului, codul sursă pe CD

Ofertantul își asumă integral atât cele 12 luni de mentenanță și suport post-implementare, cât și disponibilitatea pentru ajustări tehnice timp de 2 ani, indiferent de faptul că aceste perioade depășesc data de 31 decembrie 2026. Modalitatea administrativă de contractare a perioadei ulterioare se stabilește de comun acord, fără ca aceasta să afecteze angajamentul asumat.

13. Managementul calității

13.1 Cadrul

Managementul calității se desfășoară conform ISO 9001, așa cum cere caietul [CS §7.3, p. 43], cu două mecanisme obligatorii, aplicate fără excepție:

Registrul neconformităților — fiecare neconformitate identificată în testarea internă, în UAT sau în exploatare se înregistrează cu: descriere, severitate, modul afectat, regula sau criteriul CA-* încălcat, responsabil, termen, stare, verificarea închiderii. Registrul este vizibil beneficiarului în timp real, nu raportat periodic.

Revizia formală „patru ochi" pentru orice livrabil — niciun document, nicio modificare de cod și nicio configurație nu se predă fără verificarea unei a doua persoane cu competența necesară. Pentru cod, aceasta este integrată în procesul de dezvoltare: nicio modificare nu ajunge în ramura principală fără aprobarea unui al doilea dezvoltator.

13.2 Trasabilitatea de la cerință la dovadă

Fiecare identificator din Anexa T3 — regulă de business RB-*, criteriu de acceptanță CA-*, ecran UI-* — devine etichetă în sistemul de management al proiectului. Consecința: beneficiarul poate vedea, în orice moment, starea fiecărei reguli și a fiecărui criteriu de acceptanță — nespecificat, în dezvoltare, dezvoltat, testat, acceptat.

Aceasta transformă raportarea de progres dintr-o estimare procentuală într-o stare verificabilă pe elemente numărabile.

14. Managementul de proiect

14.1 Sistemul electronic de management

Conform cerinței [CS §7.3, p. 43], se folosește un sistem electronic de management al proiectului — JIRA, Redmine sau Azure DevOps, la alegerea beneficiarului dintre acestea — cu instanță dedicată proiectului și conturi pentru echipa beneficiarului, active din prima săptămână a Etapei I.

Ce vede beneficiarul, permanent: planul pe etape și iterații; starea fiecărei unități de lucru; registrul neconformităților; registrul riscurilor; registrul deciziilor; registrul punctelor deschise, cu responsabil și termen.

14.2 Ritmul de comunicare

Ritm	Format	Participanți
Zilnic	Sincronizare internă a echipei, 15 minute	Echipa prestatorului
Săptămânal	Raport de progres scris + ședință de coordonare	Managerul de proiect al prestatorului, punctul de contact al beneficiarului
La două săptămâni	Demonstrație a versiunii funcționale	Echipa, beneficiarul, utilizatori-cheie

Ritm	Format	Participanți
La granița de etapă	Recepție parțială documentată	Comisia de recepție
La cerere	Ședință de escaladare, în maximum 24 de ore de la solicitare	După caz

14.3 Controlul modificărilor

După aprobarea modelului TO-BE la finalul Etapei I, orice cerință nouă parcurge o procedură explicită: înregistrare, analiză de impact (efort, termen, riscuri, module afectate), decizie comună, actualizarea modelului de referință.

Procedura nu are scopul de a refuza modificările — într-un proiect cu specificație în formare, modificările sunt inevitabile și utile. Scopul este ca fiecare modificare să aibă un cost vizibil și o decizie asumată, în locul acumulării tăcute care duce la nelivrare.

15. Echipa de proiect

15.1 Componența cerută și alocarea

Documentația de atribuire cere opt roluri de specialitate, cu CV-uri, diplome sau certificări și rapoarte de muncă.

Rol	Experiență minimă cerută	Alocare Etapele I–II	Alocare Etapele III–IV	Alocare Etapele V–VI
Manager de proiect	5 ani	Plan, riscuri, relația cu AGE și STISC	Coordonare, raportare, control al modificărilor	Tranziție, raportare de mentenanță
Arhitect de soluții	5 ani	Model TO-BE, ADR-uri, scheletul soluției	Revizie de cod, decizii tehnice	Consultanță
Analist business	3 ani	Workshopuri, dicționar de date, BPMN	Criterii de acceptanță, sprijin la UAT	Instruire
Dezvoltator backend	3 ani	Schelet, module de fundație	Modulele operative	Remedieri
Dezvoltator front-end	3 ani	Prototipuri, sistem de design	Back-office și aplicația de teren	Remedieri
Administrator baze de date	3 ani	Schemă, constrângeri, indecși	Migrare, optimizare	Backup, restaurare, întreținere
Inginer DevOps	3 ani	Integrare continuă, medii, Helm	Automatizare, observabilitate	Rollout, monitorizarea SLA
Inginer QA	3 ani	Strategia de testare	Automatizare, E2E, încărcare, securitate	Regresie

15.2 Documentele de personal

Pentru fiecare dintre cele opt roluri se depun, conform cerinței: CV-ul în format structurat, cu experiența relevantă datată și verificabilă; diploma de studii și/sau certificările profesionale relevante; raportul de muncă sau documentul echivalent care atestă raportul juridic cu ofertantul.

Documentele de personal pentru toate cele opt roluri se depun în dosarul de calificare care însoțește prezenta propunere.

15.3 Capacitatea de execuție și experiența relevantă

Documentele care atestă îndeplinirea criteriilor de calificare — experiența specifică, proiectele similare, contractul de referință și experiența în interacțiunea cu sistemele informaționale partajate instituite de Guvern (MPass, MSign, MCloud, MConnect, MNotify, MLog, conform HG nr. 822/2020) — se depun în dosarul de calificare care însoțește prezenta propunere.

Sinteza, pentru orientarea comisiei:

Criteriu	Cerință	Îndeplinire
Experiență specifică în mentenanța și dezvoltarea sistemelor informatice de complexitate majoră	minimum 3 ani, în perioada 2021–2026	*[a se completa: perioada acoperită și contractele care o atestă]*
Proiecte similare	minimum 2	*[a se completa: denumirea, beneficiarul, perioada, obiectul]*
Contract individual de referință	minimum 50% din valoarea contractului atribuit	*[a se completa: beneficiarul, perioada, valoarea, actul doveditor anexat]*
Interacțiunea cu sistemele informaționale partajate instituite de Guvern	demonstrată	*[a se completa: platformele, proiectele și rolul ofertantului]*
Personal de specialitate	8 roluri, cu CV, diplome/certificări și rapoarte de muncă	Dosarul de personal, anexat

Acolo unde un criteriu se acoperă prin asociere, subcontractare sau terț susținător, conform Legii nr. 131/2015, angajamentul corespunzător este anexat la dosar, iar rolul fiecărei părți în executarea contractului este descris explicit.

15.4 Continuitatea echipei

Ofertantul se angajează ca persoanele nominalizate să fie cele care execută efectiv contractul. Înlocuirea oricărui membru al echipei se face numai cu o persoană având cel puțin aceleași calificări și experiență, cu notificarea și acordul prealabil al beneficiarului.

16. Managementul riscurilor

16.1 Abordarea

Registrul riscurilor se constituie în Etapa I, se revizuiește săptămânal și este vizibil beneficiarului în sistemul de management al proiectului. Fiecare risc are: descriere, cauză, efect, probabilitate, impact, măsură de reducere, responsabil, indicator de declanșare.

Ofertantul prezintă mai jos riscurile identificate înainte de începerea contractului, din analiza documentației. Le declară deschis pentru că un risc nedeclarat nu dispare — se materializează la recepție.

16.2 Registrul inițial

#	Risc	Impact	Măsura de reducere	Indicator de declanșare
R1	Specificația celor 14 module este subțire în caiet (4 pagini). Scopul se poate extinde nelimitat în timpul execuției.	Critic — nelivrare la termen	Anexa T3 depusă odată cu oferta, ca punct de plecare; acceptarea formală a modelului TO-BE la finalul Etapei I ca bază de referință contractuală; procedură explicită de control al modificărilor	Cerințe noi apărute după aprobarea TO-BE, în volum care depășește marja planificată
R2	**Sincronizarea offline** este cel mai mare bloc tehnic necunoscut	Major — un modul central nefuncțional în teren	Prototipare în **Etapa II**, nu descoperire în Etapa III; semantică de conflict împrumutată dintr-un model matur, nu inventată; testare pe conectivitate degradată ca activitate distinctă	Prototipul din Etapa II nu demonstrează sincronizarea corectă pe scenariile de conflict
R3	Formalitățile de conectare la AGE (Formular Unic, certificat de sistem, acces la mediile de testare) întârzie	Major — blochează M1 și semnarea	Depunere în prima săptămână a Etapei I; arhitectură cu comutare, care permite livrarea completă pe autentificare și semnare interne	Lipsa confirmării la 10 zile lucrătoare de la depunerea dosarului complet, față de termenul declarat de 7 zile lucrătoare
R4	API-urile AFIS, EVOFINDER, TRAFFIC nu sunt disponibile	Mediu — controlat contractual	Delimitare explicită în §2.1: identificatorii și arhitectura conectorilor sunt incluse; conectorii efectivi sunt condiționați. Serviciul de împachetare ANSI/NIST-ITL reduce efortul de integrare ulterioară la transport	Absența unui răspuns de la producători până la finalul Etapei II
R5	**Migrarea datelor** nu este tratată în caiet; volumul și calitatea datelor existente sunt necunoscute la ofertare	Major — poate bloca punerea în funcțiune	Analiză în Etapa I, imediat după primirea datelor; migrare idempotentă și repetabilă; zonă de carantină pentru datele neconforme; rulare în paralel	Volum sau grad de neconformitate care depășește ipotezele din Etapa I
R6	Contradicția tehnologică din caiet — se cer platforme open source fără costuri, dar Oracle și MS SQL Server sunt listate ca opțiuni	Mediu — risc de interpretare la evaluare	Ofertantul livrează integral open source, cu Anexa T2 ca dovadă. Interpretarea „fără costuri de licențe" este tratată ca cerință fermă	Solicitare de clarificare din partea comisiei
R7	**Tipărirea etichetelor** — Web Bluetooth nu este suportat în Firefox	Mic — soluție alternativă disponibilă	§7.4: restrângere pentru o singură funcție sau aplicație companion, fără cost suplimentar	Refuzul ambelor variante
R8	Cadrul normativ citat în caiet include un act din alt stat (Legea nr. 506/2004)	Mic — clarificabil	Proiectare pe Legea nr. 133/2011; confirmarea în Etapa I	—
R9	**Intervalul de execuție** — 4 luni pentru 14 module și 8 roluri	Critic	Ordine de implementare pe dependențe și risc (§11.3); suprapunerea etapelor; UAT pe module, nu la final; livrare incrementală la două săptămâni	Întârziere cumulată de peste 2 săptămâni la orice poartă de etapă
R10	Indisponibilitatea unui membru-cheie al echipei	Mediu	Documentarea deciziilor în ADR-uri și în sistemul de management; revizie „patru ochi" pe fiecare livrabil, deci cunoașterea nu este concentrată într-o singură persoană; înlocuire cu calificare echivalentă	Absență neplanificată de peste 5 zile lucrătoare

Partea IV — Obligațiile post-livrare

17. Documentația

Caietul enumeră nouă livrabile de documentație, „în format digital și tipărit", redactate „în limba română, cu terminologie tehnică și juridică adecvată", declarate „proprietatea exclusivă a Beneficiarului" [CS §8.1, p. 43].

#	Livrabil	Conținut	Etapa de livrare
1	Arhitectura generală a sistemului, diagrame logice și fizice, fluxuri de date și integrare	Documentul de arhitectură, ADR-urile, diagramele de desfășurare, harta integrărilor	II, actualizat la fiecare etapă
2	Manualul de instalare și configurare	Procedura completă de desfășurare, parametrii de configurare, dependențele	V
3	Manualul de administrare	Gestionarea utilizatorilor și rolurilor, matricea de drepturi, securitatea, backupul și restaurarea, auditul, nomenclatoarele, politicile SLA	V
4	Manualul de utilizare, pentru fiecare modul funcțional	Câte un manual per modul, structurat pe ecranele UI-* din Anexa T3	IV–V, pe măsura închiderii modulelor
5	Ghidul de operare în teren și protocoalele de lucru offline	Procedura de lucru offline, sincronizarea, reconcilierea conflictelor, tipărirea etichetelor, procedura în caz de pierdere a dispozitivului	IV
6	Documentația API și specificațiile de interoperabilitate (EVOFINDER, TRAFFIC, AFIS)	Specificația OpenAPI publicată și versionată; contractele de date ale conectorilor; maparea câmp-la-câmp	III, actualizată continuu
7	Politicile de securitate și confidențialitate, inclusiv procedurile de protecție a datelor	Politicile de acces, criptare, retenție, rotația cheilor; procedurile de tratare a cererilor persoanelor vizate; evaluarea de impact; matricea controalelor ISO/IEC 27001–27005	III
8	Planul de testare și rezultatele testelor de performanță	Strategia de testare, cazurile derivate din criteriile CA-*, rapoartele de testare de performanță și securitate	II (plan), III–IV (rezultate)
9	Codul sursă în format CD	Codul complet, cu istoricul de versiuni, procedurile de compilare și inventarul de componente (SBOM)	La recepția finală

Toate livrabilele se predau atât în format digital, cât și tipărit, conform cerinței, în limba română, cu terminologie tehnică și juridică adecvată, și devin proprietatea exclusivă a beneficiarului.

Documentația se scrie pe măsura dezvoltării, nu la final. Actualizarea documentației ecranelor afectate face parte din definiția de „terminat" (§11.2).

18. Instruirea

Patru categorii de personal, cu materiale care includ „prezentări, fișe de lucru, tutoriale video și ghiduri de bune practici" [CS §8.2, p. 43].

Categorie	Conținut	Format	Etapa
Personal criminalistic de teren	Utilizarea tuturor modulelor operative: CFL, expertize, trageri, custodie, EOD, dactiloscopie. Accent pe lucrul în teren, offline, scanarea codurilor, tipărirea etichetelor	Sesiuni practice pe grupe, în unități; fișe de lucru; tutoriale video scurte pe operațiune	V
Coordonatori și personal de conducere	Repartizarea, validarea, monitorizarea SLA, tablourile de bord, rapoartele	Sesiuni dedicate; ghid de bune practici	V
Personal IT al beneficiarului	Administrarea sistemului, nomenclatoarele, matricea de drepturi, politicile SLA, backupul și restaurarea, monitorizarea, diagnosticarea incidentelor, procedurile de desfășurare	Sesiuni tehnice aprofundate, cu acces la mediul de testare; documentație de administrare	V–VI
Management	Rapoartele de conformitate și de performanță, indicatorii, interpretarea datelor	Sesiune dedicată; ghid de interpretare	V

Materialele rămân proprietatea beneficiarului și pot fi reutilizate pentru instruirea personalului nou, fără implicarea prestatorului. Tutorialele video se predau în format editabil, pentru a putea fi actualizate.

Ofertantul propune, ca element de discutat în Etapa I, formarea unui nucleu de utilizatori-formatori din unitatea-pilot: persoane instruite mai devreme și mai aprofundat, care devin primul nivel de sprijin pentru colegi. Într-un sistem cu utilizatori dispersați teritorial, aceasta este cea mai eficientă structură de adopție.

19. Mentenanța, suportul și transferul de cunoștințe

19.1 Nivelurile de serviciu

Categorie de incident	Definiție	Termen de remediere [CS §8.3]
Critic	Sistemul sau un modul esențial este indisponibil; pierdere sau alterare de date; compromiterea integrității auditului sau a lanțului de custodie; imposibilitatea de a finaliza un flux cu valoare juridică	maximum 24 de ore
Minor	Funcționalitate afectată parțial, cu soluție de ocolire disponibilă; probleme de interfață; erori de raportare fără impact operativ	maximum 5 zile lucrătoare

Clasificarea severității se stabilește de comun acord în Etapa I și se anexează la contract, pentru a evita disputele de încadrare în perioada de suport.

19.2 Canalele de suport

Sistem de ticketing securizat, cu conturi pentru personalul desemnat al beneficiarului, cu evidența completă a solicitărilor, a termenelor și a soluțiilor. Asistență online și telefonică în intervalul de lucru al beneficiarului. Actualizări de securitate lunare, plus intervenție imediată la publicarea unei vulnerabilități critice în componentele folosite — monitorizarea acestora este automatizată prin scanarea dependențelor din integrarea continuă.

19.3 Transferul de cunoștințe

Obiectivul declarat: la finalul perioadei de suport, personalul IT al beneficiarului trebuie să poată opera, configura și modifica sistemul fără prestator. Este cerința din cap. 8.3 și, deopotrivă, condiția de sustenabilitate a investiției.

Mecanismele: documentația completă (§17); sesiuni tehnice cu personalul IT, în Etapele V și VI; accesul la sistemul de management al proiectului, cu istoricul complet al deciziilor și al modificărilor; codul sursă cu istoricul de versiuni, nu doar un instantaneu final; ADR-urile, care explică de ce s-a decis fiecare alegere de arhitectură — informația care se pierde cel mai repede și costă cel mai mult să fie reconstituită.

20. Drepturile asupra rezultatelor și conformitatea de licențiere

20.1 Angajamentul privind drepturile

La finalul perioadei contractuale, beneficiarul deține toate drepturile asupra codului sursă dezvoltat, structurii și conținutului bazei de date, documentației, configurațiilor și materialelor de instruire, conform cap. 8.3 din Caietul de sarcini. Ofertantul nu își rezervă drepturi de utilizare, nu impune restricții de modificare și nu condiționează exploatarea de o relație contractuală continuă.

Codul dezvoltat de ofertant nu conține componente proprietare ale ofertantului, licențiate separat sau reutilizate din alte proiecte sub restricții. Această afirmație este verificabilă în inventarul de componente livrat cu fiecare versiune.

20.2 Conformitatea de licențiere a componentelor open source

Cerința din caiet — *„platforme OpenSource, care, la final, să nu includă costuri adiționale, cum ar fi licențe"* — este tratată ca cerință fermă, deși caietul listează, în același capitol, Oracle și MS SQL Server ca opțiuni acceptate. Ofertantul interpretează cerința de cost zero ca fiind cea determinantă și livrează integral pe componente libere.

Anexa T2 conține inventarul complet — componentă, versiune, licență, mod de utilizare, analiza implicațiilor. Principiul de selecție aplicat:

Categorie de licență	Politica ofertantului
Permisive (MIT, Apache-2.0, BSD, PostgreSQL License)	Utilizare liberă, inclusiv legare directă cu codul aplicației
LGPL	Utilizare numai prin legare dinamică, fără modificarea componentei (consumată prin managerul de pachete, fără fork). Drepturile beneficiarului asupra codului propriu nu sunt afectate
MPL-2.0	Utilizare ca serviciu separat sau prin legare, fără modificarea fișierelor sursă ale componentei
AGPL	Utilizare exclusiv ca serviciu separat, nemodificat, fără legare cu codul aplicației și fără expunerea unei versiuni modificate — cazul explicit permis de licență
Comerciale, cu abonament sau cu limitări de utilizare	**Excluse complet**

Inventarul se generează automat la fiecare livrare, ceea ce înseamnă că afirmația de conformitate rămâne verificabilă pe toată durata contractului, nu doar la momentul ofertării. Dacă o componentă își schimbă licența pe parcurs — situație reală, întâmplată recent în ecosistem — schimbarea este detectată automat și componenta se înlocuiește.

Anexa T1 — Matricea de conformitate cu Caietul de sarcini

Matricea acoperă cerințele evaluabile binar. Coloana *Dovada* indică unde se verifică îndeplinirea la recepție.

T1.1 Arhitectură și tehnologii [CS §6.1, p. 40]

Cod	Cerință din Caietul de sarcini	Conformitate	Mod de îndeplinire	Referință și dovadă
A-01	Model 3-tier cu separare strictă	**Conform**	Frontend / logică de business / date, în proiecte separate fizic	§4.1, §4.3 · Structura soluției livrate
A-02	Comunicare prin servicii RESTful JSON	**Conform**	API REST/JSON documentat OpenAPI	§4.1, §8.3 · Specificația OpenAPI publicată
A-03	HTTPS / TLS 1.3	**Conform**	TLS 1.3 obligatoriu, HSTS	§4.1, §8.1 · Configurație și scanare de securitate
A-04	100% web-based, fără instalare locală	**Conform**	SPA + PWA	§4.1 · Demonstrație la UAT
A-05	Chrome, Edge, Firefox	**Conform**	Suport complet pe toate cele trei browsere, inclusiv tipărirea etichetelor — prin driver companion acolo unde browserul nu expune interfața Bluetooth	§7.4 · Testare pe cele trei browsere
A-06	Rezoluții variate, tablete, laptopuri de teren	**Conform**	Design adaptiv; PWA optimizată pentru tabletă	§4.3 · Testare pe dispozitive
A-07	Platformă enterprise (.NET 8 / Java EE / Python FastAPI)	**Conform**	ASP.NET Core pe .NET 8 — propunerea ofertantului; platforma se poate conveni cu beneficiarul, între cele trei opțiuni admise de caiet	§4.2 · Codul sursă
A-08	SGBD relațional cu proceduri stocate și integritate referențială	**Conform**	PostgreSQL, cu chei străine reale, constrângeri și proceduri stocate; SGBD-ul se poate conveni cu beneficiarul, între opțiunile admise de caiet	§4.4 · Schema bazei de date
A-09	Open source, fără costuri adiționale de licențe	**Conform**	Stack integral open source. Cerință tratată ca fermă: orice componentă convenită ulterior se verifică față de ea	§20.2 · **Anexa T2** + SBOM generat automat

T1.2 Securitate și audit [CS §6.2, p. 40–41; §6.5, p. 41]

Cod	Cerință din Caietul de sarcini	Conformitate	Mod de îndeplinire	Referință și dovadă
S-01	Conformitate ISO/IEC 27001, 27002, 27005	**Conform**	Controalele aplicabile sunt implementate în proiectare, dezvoltare și operare; livrabilul 7	§8.1 · Politicile de securitate (livrabil 7)

Cod	Cerință din Caietul de sarcini	Conformitate	Mod de îndeplinire	Referință și dovadă
			include matricea control ISO → mecanism implementat → dovadă, astfel încât conformitatea să fie verificabilă control cu control, nu declarativă	+ matricea de controale
S-02	Criptare AES-256	**Conform**	La repaus + la nivel de câmp pentru date sensibile	§8.1 · Configurație și documentația de administrare
S-03	RBAC/ABAC cu granularitate pe rol, atribut, câmp, acțiune și stare	**Conform**	Trei niveluri de autorizare, inclusiv matricea câmp × stare	§8.2 · Anexa D din T3; test automat pe fiecare celulă
S-04	Administrare locală a utilizatorilor cu politici configurabile	**Conform**	Complexitate, expirare, blocare, istoric de parole	§8.1 · Ecranul de administrare
S-05	MPass opțional pentru SSO și MFA	**Conform**	Comutabil din configurație; MFA local independent	§2.2, §7.2 · Demonstrație în ambele moduri
S-06	Semnare prin MSign **sau** mecanisme interne	**Conform**	Model agnostic, ambele implementate	§6.6 · Demonstrație în ambele moduri
S-07	Marcă temporală și dovezi de integritate în arhive securizate	**Conform**	Marcă temporală calificată prin MSign; sigilii periodice ale jurnalului	§6.6, §6.7 · Punctul de verificare a lanțului
S-08	Audit criptat și nealterabil pentru fiecare acces, modificare, validare, semnare, export, sincronizare	**Conform**	Jurnal probatoriu append-only, cu lanț criptografic pe cheie externă	§6.7 · Raport de verificare a lanțului
S-09	Audit cu utilizator, operațiune, dată/oră, durată, rezultat, IP sursă	**Conform**	Toate câmpurile, plus rol, sesiune, stare a fluxului, valori vechi/noi	§6.7 · Structura tabelului de audit
S-10	Alerte automate de integritate la anomalii	**Conform**	Tentative de ștergere, autentificări multiple, acces neautorizat + detecție comportamentală	§6.7 · Demonstrație pe scenarii de test
S-11	Rapoarte periodice către administratorul de securitate	**Conform**	Rapoarte programate, configurabile: alertele perioadei, rezultatul verificărilor de lanț, statistica accesărilor pe rol, modificările de configurație cu impact de securitate	§6.7, §8.1 · Rapoartele generate
S-12	Principiul „patru ochi"	**Conform**	Constrângere în baza de date + flux de co-semnare	§6.6 · Test de tentativă de auto-aprobare

T1.3 Performanță și disponibilitate [CS §6.3, p. 41] · Continuitate operațională [CS §6.6, p. 42]

Cod	Cerință din Caietul de sarcini	Conformitate	Mod de îndeplinire	Referință și dovadă
P-01	Sub 3 s pentru 95% din interogările uzuale	**Conform**	Separarea raportării, indexare țintită, cache, paginare	§9.1 · Raport de testare de încărcare
P-02	Disponibilitate minimum 99,5%	**Conform**	Replici multiple, bază de date în înaltă disponibilitate, failover	§9.1 · Raport de monitorizare
P-03	Backup zilnic, criptat, locații distincte, minimum 7 versiuni	**Conform**	Automat, două locații, plus arhivare continuă a jurnalului de tranzacții	§9.1 · Configurație + raportul testării lunare
P-04	RTO maximum 6 ore	**Conform**	Procedură documentată, **testată lunar**	§9.1 · Cronometrarea exercițiului de restaurare
P-05	Indexare, particionare, arhivare automată	**Conform**	Particionare temporală pe tabelele cu creștere rapidă	§9.1 · Planul de întreținere
P-06	Cache, gestionarea conexiunilor, limitare de resurse, failover, replicare	**Conform**	Toate implementate	§9.1 · Testare de reziliență
P-07	Verificări automate și auditate ale integrității backupurilor	**Conform**	Testare automată lunară a restaurării, cu raport	§9.1 · Rapoartele lunare
P-08	Plan de continuitate și proceduri de Disaster Recovery	**Conform**	Plan pe cinci scenarii, inclusiv pierderea unui dispozitiv de teren	§9.2 · Documentul livrat

T1.4 Interoperabilitate [CS §6.4, p. 41]

Cod	Cerință din Caietul de sarcini	Conformitate	Mod de îndeplinire	Referință și dovadă
I-01	Gestionarea locală a identificatorilor externi (EVOFINDER, TRAFFIC, AFIS)	**Conform**	Atribut de primă clasă, cu validare, unicitate, jurnalizare	§7.3 · Ecranele modulelor M5, M6
I-02	Conectori REST/JSON sau SOAP, condiționat de disponibilitatea API-urilor *(condiționat)*	**Conform** — arhitectura inclusă	Interfață comună de conector; activarea efectivă condiționată de terți	§2.1, §7.3 · Contractul de conector documentat
I-03	Autentificare mutuală pe bază de certificate digitale *(obligatoriu (pentru conectorii activați))*	**Conform**	Certificate X.509, autentificare mutuală	§7.3 · Configurația conectorului
I-04	Sincronizare bidirecțională, mapare documentată, evenimente CRUD *(obligatoriu (idem))*	**Conform**	Contract de date cu mapare câmp-la-câmp	§7.3 · Documentația de interoperabilitate (livrabil 6)
I-05	Tratarea erorilor, reconciliere, arhivarea schimburilor	**Conform**	Reconciliere programată; arhivare în jurnalul inviolabil	§7.1, §7.3 · Jurnalul schimburilor
I-06	Jurnalizarea tuturor schimburilor într-un registru de audit	**Conform**	În jurnalul probatoriu	§6.7, §7.1 · Raport de audit

Cod	Cerință din Caietul de sarcini	Conformitate	Mod de îndeplinire	Referință și dovadă
I-07	Tratarea neconcordanțelor de versiune, automat sau cu intervenție controlată	**Conform**	Semantică de conflict în două grade	§6.8, §7.3 · Ecranul de reconciliere

T1.5 Metodologie și livrabile [CS §7–8, p. 42–44]

Cod	Cerință din Caietul de sarcini	Conformitate	Mod de îndeplinire	Referință și dovadă
M-01	Agile cu milestone-uri cu poartă	**Conform**	Iterații de 2 săptămâni + porți formale de etapă	§11.1
M-02	Cele 6 etape, cu recepție parțială documentată	**Conform**	Toate, cu criterii de poartă explicite	§12
M-03	Livrabilele Etapei I (AS-IS, disfuncții, TO-BE, dicționar de date, BPMN, plan de integrare)	**Conform**	Toate, plus analiza migrării	§12 / Etapa I
M-04	Aprobarea prototipurilor UI/UX de către beneficiar	**Conform**	Etapa II, pe ecranele critice	§12 / Etapa II
M-05	Testare unitară, CI, performanță, securitate, interoperabilitate, semnare	**Conform**	Plus testare de contract și testare offline	§12 / Etapa III
M-06	UAT cu rapoarte și corectare iterativă	**Conform**	UAT pe module, în paralel cu dezvoltarea	§12 / Etapa IV
M-07	Pilot într-o unitate de referință, apoi rollout național	**Conform**	Cu rulare în paralel a celor două versiuni	§12 / Etapa V
M-08	Suport post-implementare 12 luni și transfer de cunoștințe	**Conform**	Cu obiectivul ca beneficiarul să poată opera independent	§12 / Etapa VI, §19.3
M-09	Management al calității ISO 9001, registru de neconformități, revizie „patru ochi" pe orice livrabil	**Conform**	Registru vizibil beneficiarului în timp real	§13
M-10	Sistem electronic de management al proiectului, accesibil beneficiarului	**Conform**	Instanță dedicată, conturi din prima săptămână	§14.1
M-11	Cele 9 livrabile de documentație, în română, în format digital și tipărit, proprietatea exclusivă a beneficiarului	**Conform**	§17, cu etapa de livrare pentru fiecare livrabil	§17
M-12	Instruire pe 4 categorii de personal, cu materiale variate	**Conform**	Plus propunerea de nucleu de utilizatori-formatori	§18
M-13	Mentenanță: critic ≤ 24 h, minor ≤ 5 zile lucrătoare, actualizări de securitate, ticketing securizat	**Conform**	Cu clasificarea severității agreată în Etapa I	§19.1, §19.2
M-14	Beneficiarul deține toate drepturile la finalul perioadei	**Conform**	Angajament explicit, verificabil în SBOM	§20.1

T1.6 Modulele funcționale [CS §5, p. 36–40] și funcționalitatea existentă [CS §4.2, p. 5–36]

Cod	Cerință	Conformitate	Referință detaliată
F-01 … F-14	Cele 14 module funcționale	**Conform**	§5 din prezenta propunere; Anexa T3, capitolele 5–18 — domeniu, entități, stări, reguli, SLA, ecrane, criterii de acceptanță pentru fiecare modul
F-15	Portarea integrală a funcționalității existente (CFL, Expertize, Administrare, Statistici)	**Conform**	**Anexa T3**, marcaj [AS-IS §4.2] pe fiecare regulă; Anexa A din T3 — trasabilitate pagină cu pagină
F-16	Finalizarea statisticii pe expertize (marcată „pagină în lucru" în sistemul actual)	**Conform**	§5 / M12; Anexa T3, cap. 12.8

Anexa A din Anexa T3 conține matricea completă de trasabilitate a Caietului de sarcini, capitol cu capitol și pagină cu pagină, către secțiunile care tratează fiecare cerință. Ea este instrumentul cu care comisia poate verifica acoperirea integrală fără a parcurge întregul document.

Anexa T2 — Bill of materials: componente, versiuni, licențe

Inventarul componentelor terțe, cu licența și modul de utilizare. Costul de licențiere este zero pentru fiecare poziție din tabel, atât la achiziție, cât și pe durata exploatării. Se regenerează automat la fiecare livrare (SBOM în format standard) și se predă cu fiecare recepție parțială.

T2.1 Componentele soluției

Componentă	Rol în soluție	Licență	Mod de utilizare	Implicații de licențiere
ASP.NET Core	Platforma backend	MIT	Legare directă	Niciuna
ABP Framework (ediția gratuită)	Infrastructură de aplicație	LGPL-3.0	Consumat prin managerul de pachete, fără fork și fără modificare	Legare dinamică fără modificare — codul propriu rămâne integral al beneficiarului. Nu se folosesc modulele, tema sau uneltele comerciale
Entity Framework Core	Acces la date	MIT	Legare directă	Niciuna
PostgreSQL	Baza de date	PostgreSQL License (permisivă)	Serviciu	Niciuna
PostGIS	Extensie geospațială	GPL-2.0	Extensie de bază de date, neîncorporată în aplicație	Rulează în procesul bazei de date; aplicația comunică prin SQL. Nu afectează licențierea codului aplicației
Valkey *(variantă implicită)*	Cache și blocare distribuită	BSD-3-Clause	Serviciu separat	Licență permisivă, fără obligații de reciprocitate
Redis *(variantă alternativă)*	Cache și blocare distribuită	AGPL-3.0	Serviciu separat, nemodificat, fără legare cu codul aplicației	Cazul de utilizare permis de licență. Obligațiile de publicare s-ar activa doar la modificarea componentei și oferirea ei către terți — situație care nu apare în această soluție
SeaweedFS	Stocare de obiecte	Apache-2.0	Serviciu separat	Niciuna
OpenIddict	Server de autorizare	Apache-2.0	Legare directă	Niciuna
SDK MPass SAML	Autentificare federată	MIT	Legare directă	SDK oficial guvernamental
SDK MSign	Semnare electronică	MIT	Legare directă	SDK oficial guvernamental
DSS	Validarea semnăturilor, conservare pe termen lung	LGPL-2.1	Legare dinamică, fără modificare	Idem ABP
OpenBao	Gestionarea cheilor criptografice	MPL-2.0	Serviciu separat, nemodificat	MPL are copyleft pe fișier; fără modificarea fișierelor sursă, nu se declanșează
Typst	Generare PDF	Apache-2.0	Instrument separat	Suportă PDF/A
Gotenberg	Conversie de documente	MIT	Serviciu separat	Niciuna

Componentă	Rol în soluție	Licență	Mod de utilizare	Implicații de licențiere
ClosedXML	Generare XLSX	MIT	Legare directă	Niciuna
React, TypeScript, Vite	Frontend	MIT	Legare directă	Niciuna
Refine	Meta-framework de administrare	MIT	Legare directă	Niciuna
MUI	Componente de interfață	MIT	Legare directă	Se folosește pachetul de bază, nu componentele comerciale
TanStack Query	Gestionarea stării de server	MIT	Legare directă	Niciuna
Workbox	Service worker, offline	MIT	Legare directă	Niciuna
Dexie.js	Acces la stocarea locală a browserului	Apache-2.0	Legare directă	Niciuna
Apache ECharts	Vizualizări	Apache-2.0	Legare directă	Niciuna
MapLibre GL JS	Hărți	BSD-3-Clause	Legare directă	Fork liber al unei biblioteci care a trecut la licență restrictivă
ZXing.Net	Coduri de bare	Apache-2.0	Legare directă	Niciuna
BinaryKits.Zpl	Generare de etichete pentru imprimante	MIT	Legare directă	Niciuna
NFIQ 2	Evaluarea calității imaginilor dactiloscopice	Domeniu public (NIST)	Instrument separat	Standard internațional
libbiomeval	Împachetare ANSI/NIST-ITL, codare WSQ	Domeniu public (NIST)	Legare în serviciul de împachetare	Standard internațional
OpenTelemetry	Instrumentare	Apache-2.0	Legare directă	Niciuna
Prometheus	Metrici	Apache-2.0	Serviciu separat	Niciuna
Grafana	Tablouri de bord operaționale	**AGPL-3.0**	Serviciu separat, nemodificat, fără legare cu codul aplicației	Cazul explicit permis de licență. Nu se distribuie o versiune modificată; nu se încorporează cod Grafana în aplicație. Alternativă disponibilă dacă beneficiarul preferă evitarea AGPL
OpenSearch	Jurnale și replica de audit	Apache-2.0	Serviciu separat	Niciuna
Docker, Kubernetes, Helm	Rulare	Apache-2.0	Infrastructură	Niciuna

T2.2 Verificarea continuă

Inventarul de componente (SBOM) se generează automat la fiecare compilare și include: componenta, versiunea exactă, licența, dependențele tranzitive, vulnerabilitățile cunoscute. Consecințe practice pentru beneficiar:

1. Afirmația „fără costuri de licențe" rămâne verificabilă în orice moment, nu doar la ofertare.

2. O schimbare de licență a unei componente în amonte — situație reală, întâmplată de mai multe ori în ultimii ani — este detectată automat, iar componenta se înlocuiește înainte ca problema să devină contractuală.
3. Vulnerabilitățile publicate în componentele folosite sunt semnalate automat, ceea ce susține obligația de actualizări de securitate din perioada de mentenanță.

T2.3 Ce nu conține soluția

Nicio componentă cu licență comercială, cu abonament, cu limitare pe număr de utilizatori, procesoare sau instanțe, cu perioadă de evaluare, sau cu clauze care restrâng utilizarea în sectorul public. Această listă este goală prin proiectare, nu prin omisiune.

Anexa T4 — Declarații și angajamente

Prin semnarea prezentei propuneri tehnice, Societatea cu Răspundere Limitată „ITECHS", IDNO 1013600030217, reprezentată legal de administratorul Ion Prisacari, declară și se angajează:

1. **Conformitate integrală** — soluția ofertată corespunde tuturor cerințelor obligatorii din Caietul de sarcini, în modul detaliat în Anexa T1.
2. **Licențiere fără costuri** — niciun element al soluției nu generează costuri de licențiere pentru beneficiar, la achiziție sau în exploatare, conform Anexei T2.
3. **Drepturi depline ale beneficiarului** — la finalul contractului, beneficiarul deține toate drepturile asupra codului sursă, bazei de date, documentației, configurațiilor și materialelor de instruire.
4. **Echipa nominalizată** — persoanele prezentate în §15 execută efectiv contractul; înlocuirea se face numai cu calificare cel puțin echivalentă și cu acordul prealabil al beneficiarului.
5. **Ajustări tehnice timp de 2 ani** după finalizarea contractului, conform cerinței din anunțul de participare.
6. **Valabilitatea ofertei** — 90 de zile calendaristice de la data-limită de depunere.
7. **Ofertă unică, pentru întregul lot** — fără oferte alternative.
8. **Corectitudinea delimitărilor** — elementele marcate ca incluse în preț (§2) sunt executate integral; elementele marcate ca fiind condiționate de terți sunt clar identificate, fără a masca limitări.

Din partea ofertantului	Data și locul
„ITECHS” S.R.L. Ion Prisacari, administrator Semnat electronic — MoldSign	**25 august 2026** Chișinău, Republica Moldova

Digitally signed by Prisacari Ion
Date: 2026.08.25 12:34:20 EEST
Reason: MoldSign Signature
Location: Moldova
MOLDOVA EUROPEANĂ