

SMARTGOV SRL

Chișinău, Republica Moldova

PROPUNERE TEHNICĂ

pentru

**Dezvoltarea Sistemului Informațional de
Monitorizare a Stocurilor de Medicamente**

SIMSM

Beneficiar:

Agenția Medicamentului și Dispozitivelor Medicale (AMDM)

Republica Moldova

Procedura: Licitație Deschisă | CPV: 72262000-9

Valabilitate ofertă: 90 zile

Chișinău • 2026

1. Sumar Executiv.....	4
1.1. Înțelegerea Proiectului.....	4
1.2. Obiective de Business	4
1.3. Rezultate Așteptate	4
1.4. Avantajele Abordării SMARTGOV	5
2. Înțelegerea Situației Actuale.....	6
2.1. Provocări Curente.....	6
2.2. Vizibilitatea Stocurilor de Medicamente	6
2.3. Raportarea și Prognoza.....	6
2.4. Interoperabilitatea.....	6
2.5. Suportul Decizional.....	7
3. Înțelegerea Obiectivelor Licitației	8
3.1. Raportarea Zilnică Eficientă și Automatizată.....	8
3.2. Analiza Mișcărilor de Stoc și Prognoza Consumului	8
3.3. Prevenirea Penuriilor prin Alertare Preventivă	8
4. Matricea de Conformitate Tehnică	9
5. Arhitectura Soluției.....	12
5.1. Arhitectura Generală	12
5.2. Arhitectura Logică.....	12
5.3. Arhitectura Aplicației.....	12
5.3.1. Componenta API.....	12
5.3.2. Componenta FrontOffice	12
5.3.3. Componenta MConnect Events Consumer	13
5.3.4. Componenta MNotify Adapter	13
5.4. Stratul API și Integrările	13
5.5. Baza de Date.....	13
5.6. Autentificare și Autorizare	13
5.7. Jurnalizare și Monitorizare	14
5.8. Desfășurare Kubernetes.....	14
6. Stiva Tehnologică	15
7. Arhitectura Securității	17
7.1. Autentificare și Autorizare.....	17
7.2. OWASP Top 10.....	17
7.3. Gestiunea Secretelor	17
7.4. Criptare și TLS	17
7.5. Jurnalizare Audit și MLog	18
7.6. Backup și Recuperare în Caz de Dezastru	18
7.7. Managementul Vulnerabilităților și DevSecOps	18
8. Arhitectura Integrărilor.....	19
8.1. MPass – Autentificare și Autorizare	19

8.2. MConnect – Interoperabilitate Date	19
8.3. MNotify – Notificări	19
8.4. MLog – Jurnalizarea Evenimentelor de Business	20
8.5. Sisteme Externe – Nomenclator Medicamente	20
9. Metodologia de Implementare	21
9.1. Principii de Management al Proiectului	21
10. Organizarea Proiectului	23
10.1. Echipa de Implementare Propusă	23
10.2. Structura de Guvernanță	24
10.3. Matrice RACI (principalele livrabile)	24
11. Calendarul de Implementare	25
11.1. Dependențe Externe Critice	25
12. Asigurarea Calității	26
12.1. Standarde de Codare	26
12.2. Code Review	26
12.3. Analiză Statică și Dinamică	26
12.4. Release Management	26
13. Strategia de Testare	27
13.1. Testare Unitară și de Integrare	27
13.2. Testare API	27
13.3. Testare Funcțională (End-to-End)	27
13.4. Testare de Performanță	27
13.5. Testare de Securitate	27
13.6. Testare UAT și Validare Producție	28
14. Livrabile Documentare	29
14.1. Documentație Tehnică	29
14.2. Documentație Calitate și Conformitate	29
14.3. Ghiduri Utilizatori	29
14.4. Documentație MConnect (Catalogul Semantic)	30
15. Garanție și Suport	31
15.1. Categoriile de Mentenanță	31
15.2. Niveluri de Servicii (SLA)	31
15.3. Mecanisme de Suport	31
16. Managementul Riscurilor	33
17. Avantajele SMARTGOV SRL	34
17.1. Experiența în Platforme Digitale Guvernamentale	34
17.2. Certificări și Standarde de Calitate	34
17.3. Aliniamentul Stivei Tehnologice	34
17.4. Localizare și Disponibilitate	35

1. Sumar Executiv

SMARTGOV SRL prezintă această propunere tehnică în răspuns la procedura de licitație deschisă organizată de Agenția Medicamentului și Dispozitivelor Medicale (AMDM) pentru dezvoltarea Sistemului Informațional de Monitorizare a Stocurilor de Medicamente (SIMSM). Propunerea a fost elaborată pe baza Caietului de sarcini SIMSM și a întregii documentații de atribuire, cu respectarea integrală a cerințelor tehnice și funcționale specificate.

1.1. Înțelegerea Proiectului

SIMSM reprezintă o soluție tehnologică de stat, centralizată, destinată evidenței și supravegherii disponibilității medicamentelor pe întregul teritoriu al Republicii Moldova. În contextul actual, colectarea datelor despre piața farmaceutică se realizează ad-hoc și manual, SIMSM urmând să intervină ca mecanism modern și automatizat de consolidare a informațiilor.

Sistemul va monitoriza întregul lanț de aprovizionare: producători autohtoni, importatori, distribuitori angro, farmacii comunitare și instituții medico-sanitare (IMS) publice și private. Prin integrarea cu infrastructura guvernamentală digitală (MPass, MConnect, MNotify, MLog, MCloud KaaS), SIMSM va deveni sursa oficială de date pentru monitorizarea stocurilor la nivel național.

1.2. Obiective de Business

- Asigurarea mecanismului de raportare zilnică automată și manuală a intrărilor, ieșirilor și soldurilor de medicamente la nivel național.
- Construirea capacității analitice pentru urmărirea mișcărilor istorice de stoc și elaborarea prognozelor de consum.
- Prevenirea penuriilor farmaceutice prin mecanisme configurabile de alertare preventivă.
- Integrarea cu ecosistemul digital guvernamental existent: MPass, MConnect, MNotify, MLog, MCloud.
- Asigurarea transparenței și accesibilității datelor pentru autoritățile publice cu atribuții legale: MS, ANSP, CNAM, Serviciul Vamal, CAPCS.

1.3. Rezultate Așteptate

- Sistem funcțional desfășurat în mediile staging și producție din MCloud KaaS, respectând termenul contractual 31.12.2026.
- API documentat (OpenAPI) pentru raportarea automatizată de către Sistemele Registratoarelor și consumul de date de MConnect.
- FrontOffice web responsive, localizat în română, rusă și engleză, conform Modelului Unitar de Design (MUD).
- Minim 10 agregări configurate, minim 10 vizualizări în tablouri de bord, minim 10 alerte/notificări active.
- Integrare completă cu MPass (SAML 2.0 / OAuth 2.0), MConnect Events, MNotify, MLog.
- Documentație completă, cod sursă complet cu drepturi de proprietate transferate Beneficiarului.
- Training pentru 5 Administratori de Sistem.
- Garanție 12 luni cu SLA definit: 1 oră răspuns / 4 ore lucrătoare rezoluție pentru incidente critice.

1.4. Avantajele Abordării SMARTGOV

SMARTGOV SRL este o companie moldovenească cu profil tehnic focusat pe platforme digitale guvernamentale, sisteme informaționale enterprise, PKI, securitate cibernetică și arhitecturi cloud-native. Compania deține certificările ISO 9001:2015 și ISO/IEC 27001:2022, demonstrând un sistem riguros de management al calității și securității informaționale. Stiva tehnologică propusă — .NET 9, Blazor, PostgreSQL cu TimescaleDB, Kubernetes, Grafana, Keycloak — este complet aliniată cu cerințele Caietului de sarcini și cu standardele ecosistemului digital guvernamental din Republica Moldova.

2. Înțelegerea Situației Actuale

Sistemul de sănătate al Republicii Moldova gestionează un lanț farmaceutic complex, implicând sute de operatori economici: producători autohtoni, importatori, distribuitori angro, rețele de farmacii comunitare și instituții medico-sanitare publice și private. Monitorizarea stocurilor de medicamente la nivel național reprezintă o necesitate critică pentru continuitatea tratamentelor și prevenirea crizelor farmaceutice.

2.1. Provocări Curente

Colectarea datelor despre piața farmaceutică se realizează în prezent ad-hoc și manual. Lipsa unui mecanism automatizat de raportare determină o serie de disfuncționalități operaționale majore:

- Absența vizibilității în timp real asupra stocurilor de medicamente la nivel de locații individuale (farmacii, depozite, spitale).
- Imposibilitatea detectării timpurii a riscurilor de penurie pentru medicamente esențiale.
- Inconsistența și lipsa standardizării datelor colectate din surse eterogene.
- Absența unui nomenclator combinat centralizat și actualizat, care să coreleze medicamentele autorizate și neautorizate.
- Capacitate limitată de analiză a tendințelor istorice de consum și de prognoză.
- Absența mecanismelor de alertare automată configurabile pentru autoritățile cu responsabilități în sănătate publică.

2.2. Vizibilitatea Stocurilor de Medicamente

În absența SIMSM, datele privind stocurile de medicamente sunt fragmentate între sistemele proprii ale operatorilor economici, fără posibilitatea agregării și comparării la nivel național sau regional. Autoritățile de reglementare (AMDM, MS, ANSP) nu dispun de o sursă unificată și verificabilă a datelor de stoc, fapt care limitează capacitatea de decizie în situații de urgență sau de deficit de medicamente esențiale.

2.3. Raportarea și Prognoza

Procesul actual de raportare implică transmiterea manuală de date în formate neunificate, cu periodicitate variabilă. Lipsa automatizării conduce la întâzieri semnificative în disponibilizarea datelor, la erori frecvente de introducere și la imposibilitatea construirii modelelor predictive fiabile. SIMSM va introduce raportarea zilnică structurată, cu posibilitate de corectare în termen de 30 zile calendaristice, și va furniza baza de date necesară pentru prognoza consumului.

2.4. Interoperabilitatea

Ecosistemul digital guvernamental din Republica Moldova a avansat semnificativ prin platformele MPass, MConnect, MNotify, MLog și MCloud. Totuși, sistemele informaționale ale sectorului farmaceutic nu sunt integrate cu aceste platforme. Soluțiile e-Rețeta și eCMND au pregătit terenul prin introducerea în MPass a ierarhiilor organizatorice pentru farmacii și IMSP-uri, fapt care va facilita direct implementarea autorizării în SIMSM fără a fi necesară crearea de noi structuri organizatorice în MPass.

2.5. Suportul Decizional

Autoritățile cu responsabilități legale în monitorizarea sănătății publice (MS, ANSP, CNAM, Serviciul Vamal, CAPCS) nu dispun în prezent de acces structurat la date operaționale privind stocurile de medicamente. SIMSM va introduce roluri de Observator și Observator Specific, cu tablouri de bord dedicate, oferind suportul decizional bazat pe date necesare exercitării atribuțiilor legale.

3. Înțelegerea Obiectivelor Licitației

Caietul de sarcini SIMSM definește trei obiective principale ale sistemului, pe care propunerea SMARTGOV SRL le adresează în mod explicit.

3.1. Raportarea Zilnică Eficientă și Automatizată

Ref. Caiet de sarcini, §1.2: "Asigurarea unui mecanism de raportare zilnică a intrărilor, ieșirilor, respectiv a soldurilor de medicamente într-un mod eficient și automatizat, acolo unde este posibil."

Soluția propusă adresează acest obiectiv prin două mecanisme complementare:

- API securizat (OAuth 2.0 Client Credentials) expus de componenta API, care permite Sistemelor Registratorilor să transmită automat rapoarte de mișcări de stoc. API-ul suportă rapoarte batch cu procesare atomică, returnând un identificator unic per raport acceptat.
- FrontOffice web responsive (Blazor) pentru raportarea manuală de către Operatorii Registratorilor, cu funcționalități de draft, validare în timp real, import din Excel și confirmare explicită a raportului.

Combinarea raportării automate prin API cu raportarea manuală prin interfața web garantează acoperirea integrală a tuturor tipurilor de Registratori, indiferent de nivelul lor de digitalizare.

3.2. Analiza Mișcărilor de Stoc și Prognoza Consumului

Ref. Caiet de sarcini, §1.2: "Asigurarea mecanismelor de analiză a mișcărilor de stoc al medicamentelor din trecut și realizarea prognozelor consumului de medicamente în viitor."

Soluția propusă utilizează PostgreSQL cu extensia TimescaleDB pentru stocarea și agregarea eficientă a seriilor temporale de stocuri. Componenta Agregator pre-calculează agregările configurate de Administratorul Sistemului pe intervale de timp (zi, săptămână, lună, an) și dimensiuni geografice (locație, localitate, regiune, național). Grafana furnizează tablourile de bord analitice cu vizualizări de tip line chart/run chart pentru evoluția stocurilor și extrapolare pentru datele viitoare. Minim 10 agregări și 10 vizualizări vor fi configurate și validate cu Beneficiarul.

3.3. Prevenirea Penuriilor prin Alertare Preventivă

Ref. Caiet de sarcini, §1.2: "Prevenirea penuriilor și a dezechilibrelor de stoc prin implementarea unor mecanisme de alertă preventivă pentru a identifica riscurile de lipsă a medicamentelor esențiale."

Componenta Dashboard & Alert Evaluator (Grafana Alerting) va evalua periodic condițiile configurate pe datele de stoc și agregări, generând notificări prin adaptorul MNotify. Minim 10 alerte vor fi configurate, incluzând obligatoriu alerta privind lipsa raportării mișcărilor de stoc în ultimele 48 ore. Parametrii de periodicitate (implicit: evaluare la 6 ore, notificare la 24 ore) și excepțiile sunt configurabile de Administratorul Sistemului fără intervenție în cod.

4. Matricea de Conformitate Tehnică

Tabelul de mai jos prezintă conformitatea soluției propuse de SMARTGOV SRL față de cerințele Caietului de sarcini SIMSM. Fiecare cerință este referențiată explicit la secțiunea corespunzătoare din documentația de atribuire.

Cerință	Referință CS	Soluție Propusă	Conformitate	Obs.
Microservicii și arhitectură componentizată	§7.1	.NET 9 microservicii: API, FrontOffice, MConnect Consumer, MNotify Adapter. Helm chart unic configurabil.	CONFORM	
Kubernetes 1.34+, desfășurare MCloud KaaS	§7.1	Helm chart pentru toate componentele specifice. Pod Security Admission "restricted". NetworkPolicy deny-all cu excepții explicite.	CONFORM	
Autentificare utilizatori exclusiv MPass SAML 2.0	§4.1, §7.4	Integrare SAML 2.0 via biblioteca .NET AGE. Single Sign-On și Single Logout. Atribute de autorizare mapate la roluri SIMSM.	CONFORM	
Autentificare sisteme client OAuth 2.0 Client Credentials	§4.1.4, §7.4	Keycloak pentru OAuth 2.0 CC Grant. client_secret hash SHA256. Validare IP. Token JWT verificabil criptografic. Expiare configurabilă (implicit 900s).	CONFORM	
Raportare automată stocuri prin API (UC40)	§4.5.1	REST API .NET 9 cu validare detaliată, procesare atomică, returnare ID raport. Suport corectare mișcări până la 30 zile.	CONFORM	
Raportare manuală stocuri (UC50)	§4.6.1	Blazor FrontOffice cu draft persistent, validare timp real, import Excel, căutare extinsă nomenclator, confirmare explicită.	CONFORM	
Sincronizare automată nomenclator combinat medicamente	§4.3.1	CronJob Kubernetes. Sincronizare nomenclator autorizat (API public) și neautorizat (API basic auth). Periodicitate configurabilă (cron expression). Import manual disponibil.	CONFORM	
Agregări configurabile dinamic (fără restart)	§4.10	TimescaleDB Continuous Aggregates + Scheduled Refresh. Minim 10 agregări. Recalculare incrementală la corecții. Snapshot-uri pentru istoricul nomenclatoarelor.	CONFORM	
Tablouri de bord gestionate dinamic (fără restart)	§4.11	Grafana embedded în FrontOffice via proxy securizat. Export/import definiții JSON. Minim 10 vizualizări. Drilldown între vizualizări.	CONFORM	
Alerte și notificări configurabile dinamic (fără restart)	§4.12	Grafana Alerting + MNotify Adapter. Minim 10 alerte. Grupare/deduplicare notificări. Alerta obligatorie 48h non-raportare.	CONFORM	
Integrare MConnect (RSUD + MConnect Events)	§7.10, §4.8	MConnect Ambassador (container AGE). Căutare RSUD la adăugare Registrator. Consum MConnect	CONFORM	

		Events pentru actualizare date companie.		
Integrare MNotify pentru notificări	§7.10	MNotify Adapter .NET apelat de Notification Sender. Notificări după IDNP/IDNO/email. Biblioteca .NET AGE utilizată.	CONFORM	
Jurnalizare evenimente business în MLog	§7.10	Biblioteca .NET AGE MLog. 6 categorii de evenimente identificate. Câmpuri standard MLog + câmpuri adiționale SIMSM.	CONFORM	
OWASP Top 10 – Web, API, Mobile	§7.4	OWASP ASVS la proiectare. SAST (Roslyn Analyzers, SonarQube) în CI/CD. DAST (OWASP ZAP) în pipeline. Penetration testing manual la acceptare.	CONFORM	
Disponibilitate înaltă (min. 2 instanțe), SLA 99.5%/lună	§7.8, §7.6	Toate componentele stateless în Deployment cu min. 2 replici. PDB, PodTopologySpreadConstraints, Anti-Affinity. Zero-downtime rolling updates.	CONFORM	
Observabilitate: OpenTelemetry, metrice, logging structurat JSON	§7.7	OpenTelemetry SDK .NET. Prometheus (metrice). Loki/Grafana (logging JSON). Traces distribuite cu TraceId/SpanId. Alerting operational pe metrice.	CONFORM	
UI WCAG 2.2 AA, responsive 480px+, localizare RO/RU/EN	§7.2	Blazor cu MudBlazor/componente MUD. i18n .NET (RESX). Testare accesibilitate NVDA/axe-core. Responsive Bootstrap/CSS grid.	CONFORM	
Performanță: răspuns 95%<3s, 99%<5s la sarcină maximă	§7.3	Indecși PostgreSQL optimizați, connection pooling (PgBouncer), cache Redis pentru date frecvente, paginare server-side, proiecție câmpuri.	CONFORM	
Cod sursă complet, drepturi de proprietate transferate Beneficiarului	§7.13	Livrare cod sursă complet (API, FrontOffice, Helm charts, teste, scripturi CI/CD). Licențe open-source. Drepturi de modificare, compilare, redistribuire fără restricții.	CONFORM	
Documentație completă în română (ghiduri, API, arhitectură)	§7.14	Ghid Admin Sistem (RO), Ghid Admin Registrator (RO/RU), Ghid Operator Registrator (RO/RU), Ghid integrare API, Documentație OpenAPI cu SwaggerUI.	CONFORM	
Metodologie Waterfall, plan încadrat în 31.12.2026	§8.1	Plan de implementare Waterfall în 5 etape (S0–S26). Jaloane formale cu acceptare Beneficiar. Toate livrabilele finalizate până în decembrie 2026.	CONFORM	
Garanție 12 luni, SLA: 1h răspuns / 4h rezoluție critice	§9.1	Garanție 12 luni de la acceptanța finală. Punct unic de contact. Rapoarte lunare. Mentenanță preventivă, corectivă, adaptivă, perfectivă.	CONFORM	
Pod Security Admission "restricted", NetworkPolicy deny-all	§7.4	securityContext non-root, readOnlyRootFilesystem, capabilities drop ALL. NetworkPolicy ingress/egress explicit per componentă.	CONFORM	

Single helm chart configurabil pentru toate mediile	§7.9	Helm chart unic cu values per mediu (staging/producție). Helm hooks pentru migrări DB. Imagini OCI în registrul MCloud.	CONFORM	
---	------	---	----------------	--

Legendă: CONFORM = cerința este adresată integral de soluția propusă.

5. Arhitectura Soluției

5.1. Arhitectura Generală

Soluția SIMSM urmează principiul de microservicii (ref. §7.1 CS), cu componente specializate, distribuite pe namespace-uri Kubernetes dedicate în MCloud KaaS. Arhitectura este concepută pentru a elimina punctele unice de defecțiune, a suporta disponibilitatea înaltă și a permite scalarea independentă a componentelor.

Componentele sistemului sunt grupate în trei planuri logice:

- Planul de prezentare: FrontOffice (Blazor Server), expus prin HTTPS via Ingress Kubernetes.
- Planul de procesare: API (.NET 9), MConnect Events Consumer, MNotify Adapter, Agregator (TimescaleDB).
- Planul de date: Reporting DB (PostgreSQL + TimescaleDB), Analytics DB (TimescaleDB hypertables), Alerting DB (PostgreSQL pentru Grafana), Cache Redis.

5.2. Arhitectura Logică

Arhitectura logică SIMSM distinge clar între componentele specifice (dezvoltate de SMARTGOV SRL) și componentele standard (produse open-source configurate).

- Componente specifice: API, FrontOffice, MConnect Events Consumer, MNotify Adapter.
- Componente standard: PostgreSQL 17, TimescaleDB, Grafana, PgBouncer, Redis, Keycloak (OAuth 2.0 pentru sisteme client).

5.3. Arhitectura Aplicației

5.3.1. Componenta API

API-ul este o aplicație ASP.NET Core 9 minimal API, desfășurată separat față de FrontOffice (ref. §6 CS). Expune endpoint-urile REST pentru:

- Raportarea automatizată a stocurilor de Sistemele Registratorilor (autentificare OAuth 2.0 CC).
- Descărcarea nomenclatorului combinat de medicamente.
- Gestiunea automată a locațiilor de stocare.
- Consumul de date de MConnect (căutare nomenclator, extragere stoc național per medicament).

Toate endpoint-urile API sunt documentate cu OpenAPI 3.0 și expun SwaggerUI în mediul staging. API-ul rulează în minim 2 replici Kubernetes cu Horizontal Pod Autoscaler.

5.3.2. Componenta FrontOffice

FrontOffice este o aplicație Blazor Server ASP.NET Core 9, care servește interfața web pentru toți utilizatorii umani: Administrator Sistem, Administrator Registrator, Operator Registrator, Observator și Observator Specific. Blazor Server a fost ales pentru:

- Compatibilitate nativă cu biblioteca de integrare .NET MPass de la AGE (SAML 2.0).
- Posibilitatea serverului de a face proxy securizat pentru traficul Grafana (tablouri de bord embedded).

- Refolosirea aceluiasi cod .NET atât pe server cât și pentru validări, fără duplicare în JavaScript.
- Suport nativ pentru localizare (RESX), responsive design și WCAG 2.2 AA.

FrontOffice proxează traficul Grafana, verificând autentificarea și autorizarea utilizatorului înainte de a permite accesul la tablourile de bord (ref. §4.11 CS).

5.3.3. Componenta MConnect Events Consumer

Componentă .NET 9 dedicată consumului de evenimente din MConnect Events. La recepționarea evenimentului de modificare a datelor unei companii, actualizează automat denumirea și statutul Registraturii corespunzător din baza de date SIMSM (ref. §4.8.2 CS). Consumul este idempotent și bazat pe retry cu exponential backoff.

5.3.4. Componenta MNotify Adapter

Componentă .NET 9 care primește notificări de la Grafana Alerting prin webhook HTTP și le transformă în formatul compatibil MNotify, transmițându-le platformei de notificări guvernamentale. Suportă notificări după IDNP, IDNO sau adresă de e-mail explicită (ref. §7.10 CS).

5.4. Stratul API și Integrările

API-ul SIMSM respectă standardele REST cu versionare semantică a endpoint-urilor. Toate operațiunile GET, HEAD, OPTIONS sunt read-only (idempotente). PUT și DELETE sunt idempotente. Validarea se face obligatoriu pe server pentru toate câmpurile. Erorile de validare sunt returnate în format detaliat, corelate cu rândurile raportului.

5.5. Baza de Date

PostgreSQL 17 cu extensia TimescaleDB este selectat ca soluție primară de date (ref. §6 CS – "bază de date standard, gratuită cu sursă deschisă"). Aceasta satisface simultan cerințele de:

- Stocare relațională standard pentru entitățile domeniului (Entity, Site, Medicine, MedicineCode, Submission, Stock).
- Serii temporale eficiente cu hypertables TimescaleDB pentru mișcările de stoc (Stock, StockDraft).
- Agregări pre-calulate cu Continuous Aggregates TimescaleDB, care se recalculează incremental la inserarea de date noi sau la corecții (ref. §4.10 CS).
- Replici de citire pentru izolarea sarcinilor analitice (tablouri de bord, alerte) față de tranzațiile de raportare.

PgBouncer asigură connection pooling la nivel de transaction pentru a maximiza eficiența conexiunilor din Kubernetes. Migrările bazei de date sunt gestionate prin Flyway (Helm hooks), asigurând compatibilitate backward și upgrade zero-downtime.

5.6. Autentificare și Autorizare

Sistemul implementează două mecanisme distincte de autentificare, conform specificațiilor Caietului de sarcini:

- Utilizatori umani: MPass SAML 2.0. Utilizatorii anonimi sunt redirecționați la MPass. Atributele de autorizare returnate (Role, REGISTRAR_OPERATOR, REGISTRAR_ADMIN

etc.) sunt mapate la rolurile SIMSM per sesiune. Single Logout inițiat din FrontOffice. Sesiuni inactice expirate la 60 minute (configurabil).

- Sisteme client: OAuth 2.0 Client Credentials Grant via Keycloak. client_secret stocat doar ca hash SHA256. Validare adresă IP la token endpoint. Token JWT verificabil criptografic fără apel la baza de date. Expiare configurabilă (implicit 900 secunde).

5.7. Jurnalizare și Monitorizare

Jurnalizarea structurată JSON este implementată prin Serilog (.NET) cu sink-uri pentru stdout/stderr (colectate de Loki). Câmpurile obligatorii includ: tip eveniment, timestamp, nivel, subcomponentă, utilizator/agent/IP, identificator obiect, detalii textuale, TraceId/SpanId/TraceFlags (ref. §7.7 CS).

Metricile sunt expuse prin OpenTelemetry SDK pe portul 9090 (intern) și colectate de Prometheus. Grafana afișează tablourile de bord operaționale. Alerte operaționale definite pe metrici tehnice.

5.8. Desfășurare Kubernetes

Sistemul este desfășurat complet prin un singur Helm chart configurabil. Structura Kubernetes include:

- Namespace dedicat per mediu (staging, producție).
- ResourceQuota și LimitRange per namespace.
- NetworkPolicy: deny-all ingress și egress cu excepții explicite per componentă.
- Pod Security Admission: profil "restricted" aplicat la nivel de namespace.
- PodDisruptionBudget pentru toate componentele stateless cu mai mult de 1 replică.
- PodTopologySpreadConstraints și PodAntiAffinity pentru distribuție pe noduri.
- CronJob-uri Kubernetes pentru task-uri periodice (sincronizare nomenclator, evaluare agregări, cleanup).
- Probes: startupProbe, readinessProbe, livenessProbe pe toate componentele.

6. Stiva Tehnologică

Stiva tehnologică propusă de SMARTGOV SRL a fost selectată în baza criteriilor impuse de Caietul de sarcini: tehnologii moderne, utilizare largă, sustenabilitate pe termen lung, minimizare complexitate și număr de limbaje, sursă deschisă/gratuită, compatibilitate cu ecosistemul guvernamental din Republica Moldova.

Tehnologie	Justificare și Aliniament cu Cerințele CS
.NET 9 / ASP.NET Core	Versiunea LTS curentă a platformei Microsoft .NET, cu suport garantat până în 2026 și beyond. ASP.NET Core furnizează HTTP pipeline performant, minimal API pentru componenta API și Blazor Server pentru FrontOffice. Biblioteca nativă .NET AGE pentru MPass, MConnect, MNotify, MLog este direct compatibilă. Cerința CS de minimizare a limbajelor de programare (§7.1) este satisfăcută: întregul stack server-side utilizează exclusiv C# / .NET.
Blazor Server	Framework Microsoft pentru UI web interactiv în C#, fără JavaScript pe partea client pentru logica aplicației. Selectat deoarece: (1) permite re folosirea bibliotecii .NET AGE pentru integrarea MPass SAML 2.0 direct în server-side; (2) permite proxy securizat server-side pentru Grafana embedded; (3) suportă nativ responsive design, localizare RESX și WCAG 2.2. Componentele UI sunt bazate pe Modelul Unitar de Design (MUD) agreat cu AGE.
PostgreSQL 17 + TimescaleDB	Baza de date relațională open-source cu cea mai largă adoptare din industrie (ref. §7.1 CS – "utilizare largă, sustenabilitate pe termen lung"). TimescaleDB extinde PostgreSQL cu hypertables pentru serii temporale de stocuri și Continuous Aggregates pentru pre-calculul eficient al agregărilor configurate. Satisface simultan cerințele de bază de date operațională (Reporting DB), analitică (Analytics DB) și alerting (Alerting DB), reducând complexitatea arhitecturii.
Kubernetes (MCloud KaaS)	Orchestrator de containere mandatat de politica "cloud-first" a Guvernului RM (HG 128/2014). MCloud KaaS oferă Kubernetes 1.34+. Helm chart-ul unic livrat de SMARTGOV SRL va fi desfășurat direct în mediile KaaS. Kubernetes asigură disponibilitatea înaltă, scalarea elastică, zero-downtime updates, health probes și NetworkPolicy.
Redis	Cache distribuit in-memory pentru reducerea latenței la citiri frecvente (nomenclatoare, date de sesiune, rezultate de căutare extinsă). Redis Cluster în Kubernetes asigură disponibilitatea înaltă fără punct unic de defecțiune. Satisface cerința de re folosire conexiuni (connection pool) și performanță la sarcini repetitive.
Keycloak	Identity and Access Management open-source utilizat exclusiv pentru OAuth 2.0 Client Credentials Grant al Sistemelor Registratorilor și MConnect. Keycloak nu este utilizat pentru autentificarea utilizatorilor umani (gestionată de MPass SAML 2.0). Satisface cerința CS §4.1.4 de autentificare sistem client cu IP binding, client_secret hashing și token JWT.
OpenTelemetry (.NET SDK)	Standard deschis (CNCF) pentru colectarea unificată de traces, metrice și logs. Selectat conform cerințelor §7.7 CS. SDK-ul .NET permite instrumentarea automată a ASP.NET Core, HttpClient, PostgreSQL și alte biblioteci. Satisface cerința de Traceld/SpanId pentru corelarea evenimentelor.
Prometheus + Grafana + Loki	Stack CNCF standard open-source pentru observabilitate. Prometheus colectează metrice. Grafana vizualizează metrice și dashboard-uri de

	business, furnizează sistemul de alerting (Grafana Alerting) cu policy-uri, canale și notificări. Loki agregă log-urile structurate JSON. Grafana este componenta "Dashboard & Alert Evaluator" din arhitectura CS §6.
GitHub + GitHub Actions	Sistemul de versionare cod și CI/CD. Pipeline-urile GitHub Actions implementează: build automat, testare unitară și de integrare, SAST (SonarQube), DAST (OWASP ZAP), construcție imagini OCI, push în registrul MCloud, deploy automat în staging cu aprobare manuală pentru producție.
Helm	Managerul de pachete Kubernetes mandatat de CS (§7.9). Helm chart-ul unic configurat per mediu via values.yaml. Helm hooks pentru migrări DB (Flyway). Versiuni imagini OCI aliniate cu versiunea chart-ului.
Docker / containere OCI	Imaginile de container sunt construite pe imagini de bază "chiseled" (Canonical) .NET 9 – imagini minimaliste fără shell, reducând suprafața de atac (ref. §7.4 CS). Containerele rulează non-root, readOnlyRootFilesystem, capabilități DROP ALL.

7. Arhitectura Securității

Securitatea SIMSM este proiectată conform principiului "security by design", aplicând cerințele §7.4 ale Caietului de sarcini și standardele OWASP. SMARTGOV SRL deține certificarea ISO/IEC 27001:2022, garantând un cadru sistematic de management al securității informaționale aplicat pe durata întregului ciclu de viață al proiectului.

7.1. Autentificare și Autorizare

- Utilizatori umani: autentificare exclusiv prin MPass SAML 2.0. Autentificare multi-factorială asigurată de MPass. Single Sign-On și Single Logout. Sesiuni inactice expirate la 60 minute (configurabil). Roluri SIMSM derivate din attributele SAML returnate per sesiune.
- Sisteme client: OAuth 2.0 Client Credentials Grant. client_secret generat client-side (JS/WASM), stocat server-side ca hash SHA256. Validare adresă IP la fiecare apel token. Token JWT auto-semnat verificabil criptografic.
- Principiu least privilege (ref. §7.4 CS): fiecare componentă, utilizator de bază de date și ServiceAccount Kubernetes are acordate exclusiv drepturile minimale necesare funcționării.
- Logica de autorizare centralizată în cod sursă, verificabilă ușor prin code review.

7.2. OWASP Top 10

Proiectarea sistemului ia în calcul explicit vulnerabilitățile OWASP Top 10 pentru Web, API și Mobile (ref. §7.4 CS). Măsurile principale includ:

- Injecție SQL: exclusiv parametri SQL via Entity Framework Core / Dapper. Fără SQL dinamic cu concatenare de șiruri.
- Autentificare compromisă: MPass MFA + expirare sesiune + SLO. OAuth 2.0 cu IP binding pentru sisteme.
- XSS: codificare automată în Blazor. CSP header strict. Validare și sanitizare input pe server.
- IDOR și control acces defectuos: autorizare bazată pe roluri cu verificare ID entitate la fiecare cerere.
- Configurații greșite de securitate: imagini chiseled, Pod Security Admission "restricted", NetworkPolicy deny-all, secrets în Kubernetes Secrets.
- Componente vulnerabile: dependențe referențiate în ultima versiune LTS, SBOM generat la fiecare build, SAST în CI/CD.

7.3. Gestiunea Secretelor

Toate secretele sistemului (parole, connection strings, chei private, credențiale API externe) sunt stocate în Kubernetes Secrets, referențiate din Helm values. Secretele sunt separate de configurații. Rotarea planificată a secretelor nu produce indisponibilitate prin mecanismul de dual-key/graceful reload.

7.4. Criptare și TLS

Toate comunicările externe și interne utilizează canale criptate. TLS minim v1.2 (ref. §7.4 CS). Comunicarea internă Kubernetes între componente se realizează prin ServiceMesh sau mutual

TLS, fără a ieși în afara clusterului. Certificate gestionate prin cert-manager (Let's Encrypt sau CA guvernamentală).

7.5. Jurnalizare Audit și MLog

Evenimentele importante din perspectivă business sunt jurnalizate în MLog (ref. §7.10 CS).

Categoriile identificate sunt:

- Modificare oricărui nomenclator (manual sau prin API).
- Setarea sau resetarea credențialelor Sistemului Registrator.
- Transmiterea automată sau confirmarea manuală a raportului de mișcări de stoc.
- Corectarea unei mișcări de stoc.
- Corectarea datei de expirare pentru un lot.
- Interogarea stocurilor inter-instituționale de un IMSP asupra stocurilor altui IMSP.

Lista finală va fi agreată cu Beneficiarul. Structura evenimentelor respectă câmpurile standard MLog cu câmpuri adiționale SIMSM.

7.6. Backup și Recuperare în Caz de Dezastru

Backup-urile bazei de date PostgreSQL se efectuează zilnic (dump complet) și continuu (WAL streaming) în depozitul de stocare MCloud. Planul de recuperare în caz de dezastru (DRP) va fi documentat și inclus în livrabile. RTO și RPO vor fi definite în colaborare cu STISC/Beneficiarul în funcție de capacitățile MCloud.

7.7. Managementul Vulnerabilităților și DevSecOps

- SAST: Roslyn Security Analyzers și SonarQube integrate în GitHub Actions pipeline la fiecare commit.
- DAST: OWASP ZAP scan automatizat la fiecare deploy în staging.
- Dependente: Dependabot pentru actualizare automată dependente cu vulnerabilități cunoscute (NVD/CVE).
- Imagini containere: Trivy scan la fiecare build. Imagini chiseled .NET fără instrumente sau shell inutile.
- Testare penetrare manuală: conform OWASP Security Testing Guide, planificată în S23-S26 (ref. Plan de testare).

8. Arhitectura Integrărilor

SIMSM se integrează cu patru servicii guvernamentale obligatorii: MPass, MConnect, MNotify și MLog. Integrările utilizează exclusiv bibliotecile oficiale .NET publicate de AGE și protocoalele standard deschise.

8.1. MPass – Autentificare și Autorizare

Ref. §7.10, §4.1 CS; HG 1090/2013.

FrontOffice utilizează biblioteca .NET AGE pentru integrarea SAML 2.0 cu MPass. Fluxul este:

- Utilizatorul anonim accesează FrontOffice și este redirecționat la MPass.
- MPass returnează un SAML Response cu atributele de identitate (IDNP, Prenume, Nume) și autorizare (Role, locații/organizații asociate).
- FrontOffice mapează atributele la rolurile SIMSM (SYSTEM_ADMIN, REGISTRAR_ADMIN, REGISTRAR_OPERATOR, OBSERVER, OBSERVER_MS, etc.).
- Ieșirea din sistem inițiază Single Logout SAML din MPass.

API-ul pentru sisteme client (Sistemele Registratorilor, MConnect) utilizează OAuth 2.0 Client Credentials Grant via Keycloak, conform cerințelor UC15 (§4.1.4 CS).

Administratorul Sistemului este înregistrat ca Administrator de Serviciu MPass după solicitarea către AGE. Autorizarea utilizatorilor (Observatori, Administratori de Registratori) este gestionată prin interfața MPass conform UC29 (§4.3.8 CS).

8.2. MConnect – Interoperabilitate Date

Ref. §7.10, §4.8, §4.3.1 CS; HG 211/2019.

- Integrarea cu RSUD (Registrul de Stat al Unităților de Drept): la adăugarea unui Registrator nou, denumirea este completată automat prin MConnect API. Resincronizare manuală disponibilă Administratorului Sistemului.
- Sincronizare nomenclator medicamente neautorizate: API privat cu autentificare basic auth, accesat prin MConnect.
- MConnect Events (Consumer): componenta dedicată .NET consumă evenimentele de modificare date companie și actualizează automat denumirea și statutul Registratorului.

Integrarea tehnică se bazează pe MConnect Ambassador (imagine container furnizată de AGE), care simplifică configurarea și certificatele de securitate la nivel tehnic.

8.3. MNotify – Notificări

Ref. §7.10 CS; HG 376/2020.

MNotify Adapter este o componentă .NET dedicată care primește notificări de la Grafana Alerting prin webhook HTTP și le transformă în apeluri MNotify API (via biblioteca .NET AGE). Suportă:

- Notificări după IDNP (persoane fizice).
- Notificări după IDNO (organizații).
- Notificări la adrese de email explicite gestionate în SIMSM.

Canalul și destinatarii notificărilor sunt configurabili din Grafana Alerting fără intervenție în cod.

8.4. MLog – Jurnalizarea Evenimentelor de Business

Ref. §7.10 CS; HG 708/2014.

Evenimentele de business critice sunt transmise în MLog prin biblioteca .NET AGE, utilizând câmpurile standard definite la nivel de MLog și câmpuri adiționale specifice SIMSM. Jurnalizarea MLog este asincronă, pentru a nu afecta performanța tranzacțiilor principale. Lista finală a evenimentelor este agreată cu Beneficiarul.

8.5. Sisteme Externe – Nomenclator Medicamente

SIMSM sincronizează periodic nomenclatorul combinat de medicamente cu:

- Nomenclatorul medicamentelor autorizate: API public, sincronizare periodică configurabilă (cron expression), timeout configurabil.
- Nomenclatorul medicamentelor neautorizate: API privat (autentificare basic auth), sincronizare periodică separată configurabilă.

CronJob-urile Kubernetes execută sincronizările la momentele configurate. Administratorul Sistemului poate iniția manual sincronizarea sau poate importa manual lista de medicamente via template Excel.

9. Metodologia de Implementare

Conform cerințelor Caietului de sarcini (§8.1), metodologia de implementare adoptată este Waterfall. Această alegere este justificată de perioada relativ scurtă de implementare (~6 luni), cerințele bine definite în caietul de sarcini și necesitatea acceptărilor formale etapizate. Proiectul este structurat în 5 etape distincte, cu participarea activă a Beneficiarului și acceptare formală la finalul fiecărei etape.

Etapă	Săptămâni	Activități și Livrabile
E1	S0 – S4	Analiză și definitivare arhitectură: înțelegerea procesului de raportare, elaborarea v1 a documentului de concordanță, definirea structurii BD și API de raportare automatizată, stabilirea agregărilor/dashboards/alerte, elaborarea planurilor de testare, estimare resurse, agreare arhitectură finală. Livrabil: Arhitectura Soluției agreată cu Beneficiarul.
E2	S5 – S12	Dezvoltare și configurare funcționalități de bază: instalare componente standard (PostgreSQL/TimescaleDB, Grafana, Keycloak, Redis), dezvoltare API raportare automată, ghid integrare v1, prototip FrontOffice, coordonare UI cu AGE (MUD), configurare agregări principale, tablouri de bord, alerte, testare funcțională inițială, prima testare de performanță. Livrabil: API funcțional în staging, prototip FrontOffice.
E3	S13 – S18	Prime integrări și funcționalități extinse: prime integrări cu Sisteme Registratori, FrontOffice complet, integrare MPass/MConnect/MNotify, configurare și ajustare toate agregările/dashboards/alerte, definire configurări și automatizări, testare funcțională fluxuri de bază. Livrabil: FrontOffice complet, integrări guvernamentale funcționale în staging.
E4	S19 – S22	Integrări Registratori și producție: continuare integrări sisteme raportoare, finalizare document concordanță, planificare testare securitate, finalizare ghiduri, testare repetată performanță, integrare MLog, instalare mediu producție. Livrabil: Sistem desfășurat în producție, raport testare performanță.
E5	S23 – S26	Training și ajustări finale: continuare integrări sisteme raportoare, testare de securitate (OWASP), aplicare ajustări tehnice și documentare, materiale training, livrare training pentru 5 Administratori de Sistem, semnare proces-verbal acceptanță finală. Livrabil: Documentație completă, training livrat, sistem în producție acceptat.

9.1. Principii de Management al Proiectului

- Punct unic de contact (SPOC) din partea SMARTGOV SRL: Project Manager.
- Ședințe de status săptămânale cu Beneficiarul (video call sau față în față).
- Raportare lunară scrisă privind progresul, riscurile și deciziile necesare.
- Controlul modificărilor: orice modificare față de cerințele inițiale este documentată, evaluată ca impact și aprobată înainte de implementare.
- Gestionarea problemelor de integrare cu AGE și STISC: incluse în planul de proiect cu termene de răspuns agreate.

10. Organizarea Proiectului

10.1. Echipa de Implementare Propusă

Conform cerințelor §8.3 ale Caietului de sarcini, echipa SMARTGOV SRL include toate rolurile obligatorii, cu experiența necesară, demonstrată prin CV-uri și contracte similare.

Rol	Experiență	Responsabilități în SIMSM
Team Leader / Manager de Proiect	19 ani	Punct de contact Beneficiar, planificare și monitorizare livrabile, gestionare riscuri, raportare, facilitare acceptări etapizate. Peste 10 proiecte IT guvernamentale finalizate, inclusiv e-Democracy (AGE), Mold-Alert, proiecte WHO și World Bank.
Analist Date	15+ ani	Definire model de date SIMSM, proiectare structură BD TimescaleDB, definire agregări (minim 10), vizualizări Grafana (minim 10), alerte și notificări (minim 10), optimizare interogări. Experiență în BI, Data Warehouse, sisteme guvernamentale.
Dezvoltator Frontend	3+ ani	Dezvoltare componente Blazor (FrontOffice): raportare manuală, vizualizare stocuri, nomenclatoare, administrare. Coordonare UI cu AGE (MUD). WCAG 2.2 AA, responsive design, localizare RO/RU/EN. Experiență demonstrată cu Blazor și ASP.NET în proiecte guvernamentale.
Dezvoltator Backend	3+ ani	Dezvoltare API .NET 9, logică business (autorizare, validare, procesare rapoarte), integrări MPass SAML 2.0, MConnect, MNotify, MLog. Experiență demonstrată în integrări cu serviciile de platformă guvernamentale.
Inginer DevOps	3+ ani	Configurare și mentenanță componente standard (PostgreSQL/TimescaleDB, Grafana, Keycloak, Redis, PgBouncer). Helm chart, CI/CD GitHub Actions, configurare Kubernetes (NetworkPolicy, RBAC, PDB, probes). Imagini OCI. Registru MCloud. Experiență dovedită în Kubernetes, cloud-native, automatizări.
Inginer Testare	4+ ani	Elaborare planuri de testare, teste funcționale automate (xUnit, Playwright), testare performanță (k6), testare API (Postman/Newman), regresie, rapoarte de testare. Certificare Automation Testing Tekwill 2023.
Inginer Securitate Cibernetică	10 ani	Analiză arhitectură din perspectivă securitate, configurare Pod Security Admission, NetworkPolicy, SAST/DAST în pipeline, testare de penetrare manuală (OWASP), remediere vulnerabilități, documentare măsuri de securitate. Experiență DevSecOps, Kubernetes Security, SAST/DAST.
Arhitect Soluție	3+ ani	Definire arhitectură finală, revizuire tehnică livrabile, garanția coerenței soluției cu cerințele CS. Peste 15 proiecte enterprise și guvernamentale.

10.2. Structura de Guvernanță

Proiectul este guvernat printr-o structură clară de responsabilități și comunicare:

- Comitet de Coordonare: Director AMDM + Project Manager SMARTGOV. Întruniri lunare sau la necesitate. Decizii strategice, modificări de scop.
- Grup de Lucru Tehnic: responsabili tehnici AMDM + echipa SMARTGOV + reprezentanți AGE/STISC. Întruniri săptămânale sau bi-săptămânale. Decizii tehnice, validarea livrabilelor.
- Punct de Contact Zilnic: Project Manager SMARTGOV ↔ Persoana desemnată AMDM. Comunicare curentă, raportare incidente.

10.3. Matrice RACI (principalele livrabile)

Livrabil	PM	Arhitect	Dev Team	AMDM	AGE/STISC
Arhitectura agreată	A	R	C	A/I	C
API funcțional în staging	A	C	R	I	I
FrontOffice complet	A	C	R	A/I	C
Integrări guvernamentale	A	R	R	C	C/A
Raport testare performanță	A	C	R	A/I	
Training Administratori	A	C	R	A	
Documentație completă	A	R	R	A	

Legendă: R = Responsabil, A = Aprobator, C = Consultat, I = Informat

11. Calendarul de Implementare

Planul de implementare SIMSM se încadrează în termenul contractual 31.12.2026, conform cerințelor §8.1 ale Caietului de sarcini. Durata totală este de 26 de săptămâni (aproximativ 6 luni), organizate în 5 etape Waterfall cu jaloane de acceptare formale.

Etapă	Perioadă	Jaloane și Livrabile Cheie	Acceptare
E1	S0–S4 (iulie 2026)	Document arhitectură finală agreat; Structura BD și API de raportare definite; Planuri de testare aprobate; Estimare resurse Kubernetes validată.	PV Etapa 1
E2	S5–S12 (aug–sept 2026)	Componente standard instalate și configurate; API raportare automată funcțional în staging; Prototip FrontOffice validat cu AGE; Primele agregări, dashboards și alerte configurate; Prima testare de performanță finalizată.	PV Etapa 2
E3	S13–S18 (oct 2026)	FrontOffice complet dezvoltat; Integrări MPass, MConnect, MNotify funcționale în staging; Toate agregările, dashboards și alertele configurate; Testare funcțională fluxuri de bază finalizată.	PV Etapa 3
E4	S19–S22 (nov 2026)	Integrare MLog finalizată; Document concordanță finalizat; Testare de performanță repetată – rezultate conforme cu cerințele CS; Sistem desfășurat în mediul de producție; Ghiduri utilizatori finalizate.	PV Etapa 4
E5	S23–S26 (dec 2026)	Testare de securitate OWASP finalizată – toate vulnerabilitățile remediate; Training livrat pentru 5 Administratori de Sistem; Documentație completă predată; Acceptanță finală semnată (PVA Final).	PVA Final

11.1. Dependențe Externe Critice

- MPass: Înregistrarea SIMSM ca serviciu în MPass și acordarea rolului de Administrator de Serviciu necesită inițiativa Beneficiarului față de AGE. Estimat: S1-S2.
- MConnect: Configurarea fluxurilor de date cu RSUD și MConnect Events necesită coordonare cu AGE. Estimat: S6-S10.
- MCloud KaaS: Provizionarea namespace-urilor Kubernetes (staging și producție) necesită solicitare către STISC. Estimat: S0-S2.
- Nomenclator medicamente: Accesul la API-ul privat pentru nomenclatorul medicamentelor neautorizate necesită credențiale de la AMDM. Estimat: S1.

Orice întârziere în rezolvarea dependențelor externe va fi documentată și impactul asupra calendarului va fi comunicat prompt Beneficiarului.

12. Asigurarea Calității

SMARTGOV SRL aplică un sistem de management al calității certificat ISO 9001:2015, garantând procese sistematice de control al calității pe durata întregului proiect.

12.1. Standarde de Codare

- C# Coding Conventions (Microsoft) aplicate uniform prin EditorConfig.
- Analizatori statici Roslyn (StyleCop, SonarAnalyzer) configurați să blocheze build-ul la violații critice.
- Naming conventions, structură proiect și organizare cod definite în Architecture Decision Records (ADR) la debutul proiectului.
- Secretele și configurațiile nu sunt permise hardcodate în cod sursă (detectate de GitHub Secret Scanning).

12.2. Code Review

- Toate modificările de cod sursă sunt integrate prin Pull Request (PR) în GitHub.
- Minim un reviewer tehnic aprobă fiecare PR înainte de merge.
- PR-urile includ descrierea modificării, tipul (feature/bugfix/security), testele adăugate și impactul asupra performanței.
- Logica de autorizare și integrările cu sistemele externe sunt revizuite de Arhitectul Soluției.

12.3. Analiză Statică și Dinamică

- SAST: SonarQube + Roslyn Analyzers în GitHub Actions la fiecare commit. Praguri de acceptare definite: 0 blockers, 0 criticals de securitate.
- DAST: OWASP ZAP scan automatizat la fiecare deploy în staging. Rapoarte incluse în documentele de acceptare.
- Dependabot: actualizare automată a dependențelor cu vulnerabilități cunoscute.
- Trivy: scan imagini container pentru CVE la fiecare build.

12.4. Release Management

- Versiuni semantice: {MajorVersion}.{YY}{MM}.{DD}.{IncrementalNumber} conform cerințelor CS §7.9.
- Fiecare build produce artefacte cu versiune distinctă. Imaginile OCI au același tag cu Helm chart-ul.
- Mediu staging: deploy automat la fiecare merge pe branch principal.
- Mediu producție: deploy manual cu aprobare explicită în GitHub Actions, precedat obligatoriu de validarea în staging.
- Rollback: Helm permite rollback la versiunea precedentă în sub 5 minute.

13. Strategia de Testare

Strategia de testare SIMSM este elaborată conform cerințelor §7.11 și §3 (Plan de testare) ale documentației de atribuire, cu accent pe testarea de performanță (volumele estimate de 3 ani de date) și pe validarea securității conform OWASP.

13.1. Testare Unitară și de Integrare

- Testare unitară: xUnit pentru toate clasele de servicii, validatori și logică business din API și FrontOffice. Acoperire minimă țintită: 80% pentru codul de business logic.
- Testare integrare: Testcontainers (Docker) pentru teste de integrare cu PostgreSQL/TimescaleDB, asigurând izolarea față de mediul de staging.
- Testele automate sunt parte din codul sursă și se execută în CI/CD la fiecare commit.

13.2. Testare API

- Colecții Postman/Newman pentru toate endpoint-urile REST expuse de API. Includ scenarii happy path, erori de validare, autentificare invalidă, procesare atomică, corectări.
- Testele API se execută automatizat în pipeline-ul GitHub Actions după fiecare deploy în staging.

13.3. Testare Funcțională (End-to-End)

- Playwright (C#) pentru testarea E2E a fluxurilor critice din FrontOffice: autentificare/autorizare, raportare manuală, vizualizare stocuri, vizualizare raportări, administrare nomenclatoare.
- Scenariile de testare funcțională sunt elaborate și agreate cu Beneficiarul în Etapa 1.
- Testare funcțională realizată etapizat conform planului: S5-S12 (fluxuri de bază), S13-S18 (fluxuri complete), S23-S26 (regresie finală).

13.4. Testare de Performanță

Testarea de performanță este o prioritate specifică SIMSM, dată fiind natura sa de sistem de raportare zilnică la scară națională. Instrumentul principal: k6 (sarcini HTTP) + TimescaleDB/Grafana (vizualizare rezultate).

- Datele de test generate corespund unui volum simulat de 3 ani: ~2,190,000 rapoarte, ~1,095,000,000 rânduri de mișcări de stoc (estimat).
- Scenarii de load testing: 20 sisteme concurente API, 100 utilizatori FrontOffice concurenți, vizualizare stocuri, vizualizare raportări, evaluare 1000 alerte/oră.
- Scenarii de stress testing: identificare limite, comportament la suprasarcină, degradare grațioasă.
- Praguri de acceptare: 95% răspunsuri < 3s, 99% < 5s; rapoarte: 90% < 5s, 99% < 10s (ref. §7.3 CS).
- Testare performanță programată: S5-S12 (validare arhitectură), S19-S22 (validare finală). Scenariile sunt agreate cu Beneficiarul în S0-S4.

13.5. Testare de Securitate

- OWASP Security Testing Guide aplicat conform §7.11 CS. Planificare în S19-S22, execuție în S23-S26.
- Testare manuală penetrare: autentificare/autorizare, injecție, IDOR, configurații greșite, gestionare sesiuni.
- Toate vulnerabilitățile identificate sunt remediate înainte de acceptanța finală.

13.6. Testare UAT și Validare Producție

- UAT: Beneficiarul (AMDM) validează fluxurile functionale critice în mediul staging înainte de acceptarea fiecărei etape.
- Validare producție: după fiecare deploy în producție, se execută smoke tests pentru a confirma funcționalitatea de bază.

14. Livrabile Documentare

Documentația SIMSM va fi elaborată în limba română (cu excepțiile specificate), în format editabil, incluzând sursele pentru toate artefactele (diagrame, imagini). Documentația este actualizată la zi pe durata perioadei de mentenanță (ref. §7.14 CS).

14.1. Documentație Tehnică

- Arhitectura Soluției: descriere componente, diagrame arhitecturale, decizii de design (ADR), justificări tehnologice.
- Modelul de Date: DDL complet PostgreSQL/TimescaleDB cu comentarii, indecși, relații, descriere câmpuri.
- Documentația API (OpenAPI 3.0): toate endpoint-urile, scheme request/response, modalitate de autentificare, exemple, SwaggerUI inclus.
- Ghid de Desfășurare: instrucțiuni Helm chart, values.yaml comentate complet, proceduri de instalare inițială și upgrade.
- Proceduri Operaționale: backup/restore, monitorizare, proceduri de recuperare în caz de dezastru (DRP), gestionare certificate.
- Documentația Jurnalizării: câmpuri logging structurat JSON per componentă, categorii de evenimente MLog.
- Documentația Metricilor de Business: descriere metrici OpenTelemetry expuse, praguri alerte operaționale.
- Estimarea Spațiului de Stocare: calcul detaliat pentru creșterea estimată a datelor în timp; ghid estimare spațiu agregări adiționale.
- Planul de Recuperare în Caz de Dezastru (DRP): proceduri, RTO, RPO, responsabilități.

14.2. Documentație Calitate și Conformitate

- Document de Concordanță: matricea de trasabilitate dintre Conceptul/Regulamentul SIMSM și soluția implementată (ref. §7.14 CS).
- Plan de Testare Funcțională și Raport de Testare Funcțională.
- Plan de Testare de Performanță și Raport de Testare a Performanței (cu instrucțiuni de executare k6).
- Documentația Măsurilor de Securitate: măsuri de proiectare, implementare și desfășurare, vulnerabilități identificate și remediate.

14.3. Ghiduri Utilizatori

- Ghid Administrator Sistem (română): configurare nomenclatoare, gestiune Registratori, gestiune agregări, tablouri de bord, alerte, notificări. Include aspecte de administrare MPass și configurări sistem.
- Materiale Training Administrator Sistem (română): prezentări, exerciții practice, ghid rapid.
- Ghid Administrator Registrator (română + rusă): gestiune locații, credențiale sistem, operatori.
- Ghid Operator Registrator (română + rusă): raportare manuală stocuri, corectări, vizualizare.
- Ghid de Integrare pentru Sistemele Registratorilor (română): autentificare OAuth 2.0, API raportare automată, descărcare nomenclator, gestiune locații. Include exemple de request/response.

14.4. Documentație MConnect (Catalogul Semantic)

Conform cerințelor §9.1 CS, SMARTGOV SRL va elabora și livra documentația tehnică de integrare necesară publicării pe platforma MConnect, va completa activele semantice aferente tuturor fluxurilor de date SIMSM și va oferi suport pentru plasarea în Catalogul Semantic Național (ref. HG 211/2019).

15. Garanție și Suport

Perioada de garanție este de 12 luni de la data semnării procesului-verbal de acceptanță finală, conform §9 al Caietului de sarcini. SMARTGOV SRL furnizează servicii complete de întreținere și suport tehnic pentru toate componentele SIMSM pe durata perioadei de garanție, fără costuri suplimentare.

15.1. Categoriile de Mentenanță

- **Mentenanță preventivă:** monitorizare continuă, verificări periodice de sănătate, actualizări de securitate (patching), verificarea mecanismelor backup/restore, optimizarea configurațiilor, verificarea integrităților.
- **Mentenanță corectivă:** remedierea erorilor, incidentelor, defectelor și comportamentelor neprevăzute ale sistemului.
- **Mentenanță adaptivă:** ajustarea sistemului la modificări ale infrastructurii MCloud/KaaS, servicii guvernamentale, nomenclatoare, cadru normativ.
- **Mentenanță perfectivă:** optimizări minore de performanță, securitate, utilizabilitate și observabilitate, fără modificarea domeniului funcțional aprobat.

15.2. Niveluri de Servicii (SLA)

Severitate	TimP Răspuns	TimP Rezoluție	Descriere
Critic	≤ 1 oră	≤ 4 ore lucrătoare	Sistem indisponibil sau raportare blocată la nivel național; pierdere date; vulnerabilitate critică de securitate.
Major	≤ 4 ore	≤ 1 zi lucrătoare	Funcționalitate principală degradată; API neperformant; integrare guvernamentală nefuncțională.
Mediu	≤ 8 ore	≤ 2 zile lucrătoare	Funcționalitate secundară afectată; erori izolate; degradare parțială a performanței.
Minor	≤ 8 ore	≤ 5 zile lucrătoare	Erori cosmetice; solicitări de informații; optimizări minore.

15.3. Mecanisme de Suport

- **Punct unic de contact (SPOC):** adresă email dedicată și mecanism electronic de înregistrare și urmărire a solicitărilor.
- **Rapoarte lunare:** lista incidentelor, respectarea SLA, disponibilitatea sistemului, modificări aplicate, vulnerabilități remediate, recomandări.
- **Analiza cauzei rădăcină (RCA)** pentru incidente critice și majore, cu plan de acțiuni preventive.
- **Transfer de cunoștințe:** sesiuni de instruire punctuală la livrarea modificărilor cu impact operațional.

- Ferestre de mentenanță: intervențiile planificate se execută în ferestre agreate cu Beneficiarul, comunicate în prealabil.
- Documentație MConnect: elaborare documentație integrare și publicare pe MConnect conform HG 211/2019.

16. Managementul Riscurilor

Risc	Probab.	Impact	Măsuri de Atenuare
Întârzieri în configurarea MPass de către AGE	Mediu	Major	Inițierea solicitării de înregistrare SIMSM în MPass în S0, anterior startului efectiv al dezvoltării. SMARTGOV SRL include un mecanism de autentificare mock pentru testare paralelă.
Întârzieri în provizionarea MCloud KaaS (STISC)	Mediu	Major	Solicitare namespace-uri Kubernetes în S0. Utilizarea unui cluster Kubernetes local (k3s) pentru dezvoltare și testare inițială paralelă cu provizionarea.
Acces întârziat la API nomenclator neautorizat (credențiale AMDM)	Scăzut	Mediu	Solicitare credențiale în S0. Mecanismul de sincronizare este proiectat modular; până la obținerea credențialelor, componenta poate fi testată cu date mock.
Complexitate integrare MConnect Events (evenimente de companii)	Mediu	Scăzut	SMARTGOV SRL are experiență directă cu MConnect Events (proiecte anterioare). Utilizarea MConnect Ambassador (image AGE). Testare integrare planificată în S6-S10.
Performanță insuficientă la volume mari (TimescaleDB, Grafana)	Mediu	Major	Prima testare de performanță în S5-S12 pe date generate (3 ani). Indexuri, Continuous Aggregates, replici de citire. Ajustări iterative până la îndeplinirea cerințelor §7.3 CS.
Vulnerabilități de securitate identificate târziu	Scăzut	Critic	SAST/DAST continuu în CI/CD din S0. Pod Security Admission și NetworkPolicy aplicate din prima desfășurare. Testare penetrare planificată în S23-S26, cu suficient timp de remediere.
Modificări de scop sau cerințe suplimentare din partea Beneficiarului	Mediu	Mediu	Procedura formală de gestionare a modificărilor (Change Management). Orice cerință suplimentară este tratată ca solicitare separată, cu analiză impact și aprobare.
Disponibilitate Registratori pentru integrare și testare	Mediu	Scăzut	Ghid de integrare v1 livrat în S5-S12. Mediu sandbox disponibil pentru testare integrare. Suport tehnic dedicat Sistemelor Registratorilor în S13-S26.

17. Avantajele SMARTGOV SRL

SMARTGOV SRL este o companie din Republica Moldova specializată în platforme digitale guvernamentale, sisteme informaționale enterprise, securitate cibernetică, PKI și arhitecturi cloud-native. Această secțiune prezintă experiența relevantă demonstrată prin contracte finalizate, care susține direct capacitatea de livrare a SIMSM.

17.1. Experiența în Platforme Digitale Guvernamentale

- Platforma e-Democracy (AGE, Republica Moldova): participare ca subcontractor în dezvoltarea platformei de guvernare electronică a Agenției de Guvernare Electronică. Valoare contract: 2,730,000 MDL, durata 6 luni. Relevanță directă: cunoașterea ecosistemului AGE (MPass, MConnect, MUD), procese de lucru cu AGE, standarde tehnice guvernamentale.
- Platformă de afișare date votare în timp real (UNDP Moldova / CEC, Republica Moldova): dezvoltare platformă de agregare și vizualizare în timp real a datelor dezagregate per regiune, localitate, gen și vârstă. Valoare: 1,650,000 MDL, durata 2 luni. Relevanță directă: sistem de raportare și vizualizare date în timp real la scară națională – similar arhitectural cu SIMSM.
- Analiză funcțională și evaluare arhitectură SIA AMP și SIA AMS (UCIMPS / Ministerul Sănătății, Republica Moldova): analiză funcțională, evaluarea arhitecturii și elaborarea recomandărilor de modernizare a sistemelor informaționale din domeniul sănătății. Valoare: 696,000 MDL, durata 2 luni. Relevanță directă: domeniu sănătate/medicamente, cunoașterea sistemelor informaționale MS.
- Trust Service Platform (Semnaturescu SRL, România): dezvoltarea unei platforme PKI enterprise cu semnătură electronică, identitate digitală și servicii de încredere. Valoare: 145,000 EUR, durata 12 luni. Relevanță: sisteme enterprise de înaltă securitate, autentificare și identitate digitală.

17.2. Certificări și Standarde de Calitate

- ISO 9001:2015 (Systema Certificari, valabil până 29 aprilie 2029): Management al Calității pentru servicii IT de consultanță, dezvoltare software, soluții digitale pentru e-government și infrastructuri critice.
- ISO/IEC 27001:2022 (Systema Certificari, valabil până 29 aprilie 2029): Management al Securității Informaționale. Statement of Applicability (SOA) din 02.03.2026. Garantează un cadru formal de securitate aplicabil direct pentru SIMSM.

17.3. Aliniamentul Stivei Tehnologice

Stiva tehnologică SMARTGOV SRL (.NET 9, Blazor, PostgreSQL, Kubernetes, Docker, RabbitMQ, Redis, Keycloak, OpenTelemetry, Prometheus, Grafana, GitHub, Azure DevOps) corespunde integral cerințelor Caietului de sarcini SIMSM și ecosistemului tehnologic guvernamental din Republica Moldova:

- Biblioteca .NET nativă AGE pentru MPass, MConnect, MNotify, MLog este utilizată curent de echipa SMARTGOV SRL.
- Experiența directă cu MPass SAML 2.0, MConnect API și MConnect Events este demonstrată prin proiectele finalizate.
- Kubernetes și cloud-native sunt competențe centrale ale echipei, cu over 8 proiecte de referință.

- PostgreSQL/TimescaleDB, Grafana și stiva de observabilitate sunt tehnologii utilizate activ în producție de echipa propusă.

17.4. Localizare și Disponibilitate

Ca companie din Republica Moldova, SMARTGOV SRL are disponibilitate imediată pentru:

- Întruniri față în față cu Beneficiarul (AMDM) și cu AGE/STISC la Chișinău.
- Fus orar identic cu Beneficiarul – eliminând fricțiunile de coordonare tipice proiectelor cu furnizori externi.
- Cunoașterea contextului normativ și instituțional din Republica Moldova (HG, legi aplicabile sectorului farmaceutic și IT).
- Capacitatea de asistență on-site la necesitate pe durata implementării și perioadei de garanție.

SMARTGOV SRL declară că toate informațiile tehnice prezentate în această propunere sunt exacte și verificabile, că deține competențele și resursele necesare pentru livrarea integrală a SIMSM în conformitate cu Caietul de sarcini și că se angajează să respecte toate cerințele tehnice, funcționale și de calitate specificate în documentația de atribuire.

Gheorghe PANTAZ

Administrator | SMARTGOV SRL

Chișinău, Republica Moldova, 2026