04 - Anexa 22: Technical Specification and Technical Proposal

Date: 23 June 2026
Procedure: ocds-b3wdp1-MD-1779798670296
Object: Development of the Information System for Monitoring Medicine Stocks (SIMSM)
Bidder: Varnix Technologies ltd.

Anexa 22 - Technical Specification Table

Goods / services	Model / service name	Country of origin	Producer / provider	Technical specification requested by authority	Technical specification proposed by bidder	Reference standards
Lot 1 - Development of the Information System for Monitoring Medicine Stocks (SIMSM)	SIMSM solution development and implementation services	Bulgaria	Varnix	According to the SIMSM Terms of Reference and tender documentation	Varnix proposes to deliver a cloud-native SIMSM solution covering API-based and manual reporting, FrontOffice, configurable dashboards, aggregations, alerts, government platform integrations, Kubernetes deployment, testing, documentation, training and 12-month warranty/maintenance as detailed in this technical proposal.	OpenAPI, OAuth 2.0, SAML 2.0, TLS 1.2+, OWASP Top 10, WCAG 2.2 AA, Kubernetes, OpenTelemetry, MUD principles
TOTAL					Compliant with the Terms of Reference	

1. Executive summary

Varnix proposes to design, develop, configure, deploy and support SIMSM as a centralized state information system for monitoring medicine stocks across the Republic of Moldova. The solution will automate and consolidate daily medicine stock movement reporting, support manual reporting where required, provide API access for registrar systems and MConnect, and deliver configurable aggregation, dashboard, alert and notification capabilities.

The proposal follows the tender requirement for a short implementation period and is structured around a 26-week delivery plan with formal deliverable acceptance at each phase. Varnix will deliver the configured system in staging and production, complete source code, performance tests and execution instructions, test plans and reports, system documentation, training for five system administrators and twelve months of warranty/maintenance.

2. Proposed solution components

Component	Purpose
SIMSM API Gateway and Backend Services	REST APIs for automated reporting, medicine and stock queries, credential management, registrar integration, MConnect data access and internal business workflows.
FrontOffice Web Application	Role-based web application for system administrators, registrar administrators, registrar operators, observers and specific observers, including manual stock reporting, stock views, reports, configuration and dashboards.
Reporting Database	Transactional storage for registrar data, stock movements, reports, credentials, audit history, nomenclatures and operational state.
Aggregation and Analytics Layer	Configurable aggregation jobs and analytical data structures to support dashboards, stock analytics and alert evaluation efficiently.
Dashboard and Alert Evaluator	Dynamic configuration of aggregations, dashboards, alert rules and notification templates without code changes or component restarts where required by the Terms of Reference.
Notification Adapter	Integration with MNotify and configurable notification channels/templates.

Government Platform Integration Adapters	MPass/SAML 2.0, MConnect APIs/events, MNotify, MLog and MCloud/KaaS deployment integration.
DevOps and Observability Package	Container images, a configurable Helm chart, CI/CD scripts, health checks, structured JSON logging, OpenTelemetry metrics and deployment documentation.

3. Technology stack

Area	Proposed technology / approach
Application backend	Java/Spring Boot or Node.js/NestJS, final stack to be confirmed at architecture stage
Frontend	React/Angular/Vue with MUD-aligned UI kit and WCAG 2.2 AA practices
Transactional DB	PostgreSQL with HA-ready deployment pattern on MCloud/KaaS
Analytics/aggregation	PostgreSQL materialized views and/or ClickHouse/Timescale-compatible analytical layer, selected after sizing validation
Dashboards	Configurable dashboard layer using open-source standard components where feasible; custom embedding and access control in SIMSM
Messaging/jobs	Scheduled jobs and event consumers for nomenclature sync, MConnect Events, aggregations and alerts
Containerization	Docker/OCI images deployed by a configurable Helm chart
Observability	Structured JSON logs, OpenTelemetry metrics, health checks and MLog integration

4. Functional coverage

Requirement area	Varnix implementation approach
Authentication and authorization	MPass/SAML 2.0 for users; role mapping based on returned attributes; role selection where multiple roles exist; session handling and single logout; OAuth 2.0 Client Credentials for registrar systems and MConnect.
System administrator functions	Nomenclatures, registrars, correction requests, dynamic aggregations, dashboards, alerts, notification templates and configuration management.
Registrar administrator functions	Storage location management, system credentials and IP ranges, operator authorization through MPass as per existing government mechanisms.
Registrar system API	Automated stock movement reporting, recent report listing, report details, recent stock movement details, combined nomenclature download and automatic location management.
Manual stock reporting	Manual reporting flow for registrar operators, unfinished reports, validation errors, save/submit workflow, corrections within configured period and correction requests for batch expiry dates.
Observer functions	General and specific dashboards, stock views and controlled access to national/regional data.
MConnect access	API exposure for MConnect, medicine search and national stock extraction for medicines by code, subject to final API approval.
Common functions	Stock view, stock verification for IMSP roles, report viewing, filtering, history and user-friendly error handling.

5. Security and access control

- Least-privilege access model based on tender-defined roles and MPass authorization attributes.
- OAuth 2.0 Client Credentials for machine clients with client_id/client_secret sent through headers only, IP validation and cryptographically verifiable access tokens.
- TLS 1.2 or higher for all external and internal interfaces where applicable.
- Container security aligned with Kubernetes restricted Pod Security Admission and deny-all NetworkPolicy baseline, with explicit allow rules only.
- Secure secret management aligned with MCloud/KaaS procedures.
- OWASP Top 10 oriented design and testing with special focus on authentication, authorization and access to stock data by role.
- Structured security event logging and integration with MLog for required audit events.

6. Performance and scalability

The solution will be designed and tested against the nominal volumes and response-time thresholds defined by the Terms of Reference, including approximately 1,500 users, 2,000 storage locations, up to 500 client systems, 2,000 stock reports per day, average reports of 500 rows and estimated maximum reports of 2,000 rows, 1,000 active alerts evaluated hourly and up to 10,000 notifications per day.

- Performance test data will simulate an estimated three-year operational volume.
- Database indexes, partitioning/materialization and aggregation strategies will be validated during Week 5-12 and Week 19-22 performance cycles.
- Response time targets will be verified for API reporting, manual reporting, stock views, reports, dashboard reads and alert evaluation.
- Horizontal scaling and high availability will be supported for applicable services with at least two instances for main components.

7. User interface and accessibility

- Responsive web interface usable from 480px screen width upward.
- Localization-ready interface in Romanian, Russian and English; Romanian default for production delivery.
- WCAG 2.2 AA oriented design for custom UI components.
- Alignment with Moldovan Government Modelul Unitar de Design (MUD) principles and AGE coordination for custom SIMSM UI.
- Search fields designed to ignore capitalization and diacritics where required.
- Human-readable URLs, bookmarkable search pages and visible support contact information.

8. Deployment, environments and automation

- Deployment to MCloud/KaaS in staging and production environments.
- All custom components containerized as OCI-compatible images.
- Installation and configuration through one configurable Helm chart.
- CI/CD scripts for build, test and deployment automation, subject to AMDM/STISC procedures.
- Structured JSON logs and OpenTelemetry metrics for application observability.
- Backup/restore and disaster recovery documentation prepared as part of final documentation.

9. Deliverables

Deliverable	Description
Configured system in staging and production	SIMSM deployed and configured according to the Terms of Reference and accepted implementation plan.
Complete source code	Full source code for custom components, including performance tests and execution instructions.
Testing package	Test plans, functional test reports, performance test reports, security testing report and remediation log.
Documentation package	Data model, OpenAPI documentation, compliance matrix, security measures, logging and metrics, disaster recovery plan, admin guide, training materials, registrar administrator/operator guides and integration guide.
Training	Training for five system administrators covering configuration, use, aggregations, dashboards, alerts and notifications.
Warranty and maintenance	Twelve months of maintenance and technical support after final acceptance.

10. Compliance matrix

Tender requirement group	Compliance	Varnix response
Functional use cases	Compliant	Covered through the SIMSM API, FrontOffice, role-based access, reporting, stock views, dashboards, alerts and MConnect integration.
Government integrations	Compliant	MPass, MConnect, MNotify, MLog and MCloud/KaaS are included, subject to access and support from platform owners.
Kubernetes and HA	Compliant	Containerized microservice-oriented deployment with Helm chart, HA-ready services and no intentional single point of failure in custom components.
Security	Compliant	OAuth2, SAML2, TLS, least privilege, OWASP-oriented testing, network restrictions and secure logging are included.
Performance testing	Compliant	Initial and repeated performance testing with three-year data simulation and tuning cycles are included.
Documentation and training	Compliant	Full documentation package and training for five administrators are included.
Maintenance	Compliant	Twelve-month warranty/maintenance with incident handling and monthly reporting is included.

11. Dependencies and client responsibilities

Client-facing assumptions and dependencies are listed in the separate Assumptions and Clarifications document and are incorporated into this proposal by reference. The most critical dependencies are timely access to government platforms, MCloud/KaaS resources, stakeholder decisions, test data and registrar integration counterparts.