

I. Caiet de sarcini

Servicii de mentenanță, suport tehnic și administrare

Sistemul Informațional e-Consulat

1. Scopul general

Asigurarea funcționării continue, eficiente și sigure a Sistemului Informațional **e-Consulat**, inclusiv suport tehnic, mentenanță, administrare tehnică și securitate cibernetică, în vederea susținerii activităților Ministerului Afacerilor Externe (MAE) și ale Misiunilor Diplomatice și Oficiilor Consulare (MDOC).

2. Obiective

Prestatorul va asigura:

- disponibilitatea și funcționarea continuă a sistemului;
- suport tehnic prompt pentru utilizatori și administratori;
- menținerea securității cibernetice și operaționale a sistemului;
- monitorizarea permanentă a infrastructurii și aplicației;
- remedierea rapidă a incidentelor tehnice;
- optimizarea funcționării sistemului.

3. Structura serviciilor de mentenanță

3.1. Servicii de mentenanță preventivă

Servicii planificate, executate periodic, destinate menținerii funcționării optime a sistemelor informatice:

- monitorizare infrastructură și aplicații;
- actualizări software și patch-uri de securitate;
- verificări periodice (backup, loguri, performanță);
- optimizări și mentenanță proactivă.

3.2. Servicii de mentenanță corectivă

Servicii de intervenție pentru remedierea incidentelor și disfuncționalităților apărute:

- diagnosticare și remediere incidente;
- suport tehnic utilizatori;
- restabilire funcționalitate servicii;
- intervenții de urgență.

3.3. Servicii de mentenanță adaptivă

Servicii necesare adaptării sistemelor informatice la modificări de mediu, cerințe sau integrare:

- modificări de configurații;
- adaptări la schimbări legislative / organizaționale;

- integrare cu alte sisteme;
- ajustări funcționale minore.

3.4. Servicii de mentenanță evolutivă

Servicii care implică extinderea funcționalităților existente sau dezvoltarea de noi componente:

- dezvoltările de funcționalități noi;
- dezvoltare de module noi;
- modificări majore de funcționalitate;
- automatizări complexe;
- integrații avansate / API.

4. Gestionare și mentenanță tehnică

Prestatorul va asigura:

- supravegherea permanentă a funcționării sistemului;
- monitorizarea componentelor sistemului de operare și software;
- identificarea și remedierea incidentelor;
- restabilirea funcționalității sistemului în regim de urgență;
- gestionarea actualizărilor tehnice ale sistemului de operare și aplicației;
- gestionarea bazelor de date și a serviciilor aplicației;
- menținerea integrității și disponibilității datelor.

5. Suport tehnic și punct unic de contact

Prestatorul va asigura:

- un punct unic de contact (Single Point of Contact) disponibil 24/7;
- raportarea incidentelor prin telefon, e-mail sau sistem de ticketing;
- informarea utilizatorilor privind progresul soluționării incidentelor;
- mecanism standardizat de escaladare a incidentelor;
- sistem de ticketing pentru evidența solicitărilor.

6. Mentenanță corectivă

Mentenanța corectivă include:

- diagnosticarea incidentelor raportate;
- remedierea erorilor software;
- corectarea bug-urilor;
- rezolvarea problemelor de integrare cu sisteme externe (MPass, MPay, MSign etc.);
- aplicarea patch-urilor urgente;

- testarea regresivă după remedierea incidentelor.

Scopul este reducerea timpului de indisponibilitate a sistemului și menținerea continuității serviciilor consulare.

7. Mentenanță preventivă

Mentenanța preventivă include:

- aplicarea patch-urilor de securitate;
- actualizarea componentelor software;
- verificarea periodică a integrității bazelor de date;
- verificarea mecanismelor de backup;
- monitorizarea performanței sistemului;
- generarea semestrială a rapoartelor de sănătate ale sistemului.

8. Backup și continuitatea serviciilor

Prestatorul va asigura:

- realizarea copiilor de rezervă pentru sistem, baze de date și cod;
- verificarea periodică a integrității backup-urilor;
- testarea procedurilor de restaurare;
- documentarea procedurilor de Disaster Recovery;
- restabilirea funcționării sistemului în caz de incident major.

9. Niveluri de servicii (SLA)

Prestatorul va asigura funcționarea continuă a sistemului și suportul tehnic conform următorilor indicatori minimi de performanță:

Disponibilitatea minimă a sistemelor: 99% lunar, excluzând ferestrele planificate de mentenanță.

Clasificarea incidentelor

Nivel	Descriere	Timp reacție	Timp remediere
Critic	Sistem indisponibil total	30 min	2 ore
Major	Funcționalitate esențială afectată	1 oră	4 ore
Minor	Probleme necritice	4 ore	24 ore

Prestatorul va prezenta **rapoarte lunare SLA**.

10. Securitate cibernetică

Prestatorul va asigura:

- aplicarea patch-urilor de securitate;
- monitorizarea vulnerabilităților;
- configurarea firewall-urilor;
- accesul exclusiv de la adrese IP autorizate și documentate.

- prevenirea accesului neautorizat;
- monitorizarea accesului la sistem;
- auditarea periodică, cel puțin semestrial a logurilor.

11. Controlul accesului și autentificare

Prestatorul va asigura:

- autentificarea utilizatorilor prin MPass;
- utilizarea parolelor doar în situații excepționale;
- parole complexe (minim 8 caractere);
- blocarea conturilor după încercări nereușite de autentificare;
- schimbarea periodică a parolelor, cel puțin odată la 3 luni.

12. Controlul accesului administrativ

Prestatorul va asigura:

- utilizarea conturilor individuale de administrator;
- interzicerea conturilor administrative comune;
- jurnalizarea activităților administratorilor;
- identificarea fiecărei acțiuni administrative;
- acces administrativ doar prin conexiuni securizate.
- autentificarea administratorilor prin MPass;
- utilizarea parolelor doar în situații excepționale;
- parole complexe (minim 12 caractere);
- blocarea conturilor după încercări nereușite de autentificare;
- schimbarea periodică a parolelor, cel puțin odată la 12 luni.

13. Evidența infrastructurii și conexiunilor

Prestatorul va menține registre actualizate privind:

- adresele IP utilizate;
- IP-urile publice și interne;
- porturile și serviciile deschise;
- conexiunile externe ale sistemului;
- IP-urile utilizate de personalul tehnic pentru administrare.

14. Jurnalizare și audit

Sistemul va asigura:

- jurnalizarea activităților utilizatorilor;

- jurnalizarea autentificărilor;
- jurnalizarea operațiunilor administrative;
- păstrarea logurilor minimum 6 luni;
- protecția logurilor împotriva modificării.

15. Documentare tehnică

Prestatorul va furniza și actualiza permanent:

- arhitectura sistemului;
- diagrame tehnice;
- descrierea infrastructurii;
- manuale de utilizare;
- ghiduri de administrare;
- registrele adreselor IP și conexiunilor;
- proceduri de backup și restaurare;
- codul sursă și pachetul de instalare.

16. Raportare periodică

Prestatorul va transmite lunar:

- raport privind incidentele;
- raport SLA;
- recomandări tehnice;
- statistici privind utilizarea sistemului.

Prestatorul va transmite semestrial:

- rapoartele de sănătate ale sistemului

17. Proprietate intelectuală

Codul sursă, documentația tehnică și toate modificările realizate în cadrul contractului vor aparține beneficiarului.

18. Obligațiile părților

Prestator

- asigurarea personalului calificat;
- respectarea SLA;
- respectarea cerințelor de securitate;
- documentarea activităților.

Beneficiar

- asigurarea accesului la infrastructură;

- coordonarea tehnică;
- furnizarea informațiilor necesare.

19. Confidențialitatea informațiilor

Prestatorul este obligat să asigure confidențialitatea tuturor informațiilor la care are acces în cadrul executării prezentului contract.

Prestatorul se obligă:

- să nu divulge informațiile tehnice, operaționale sau datele prelucrate în sistem către terți fără acordul beneficiarului;
- să utilizeze informațiile accesate exclusiv în scopul executării contractului;
- să asigure că personalul implicat în prestarea serviciilor respectă obligațiile de confidențialitate;
- să implementeze măsuri adecvate de protecție a datelor și informațiilor;
- să nu copieze sau extragă date din sistem fără autorizarea beneficiarului;
- să notifice imediat beneficiarul în cazul producerii unui incident de securitate sau scurgeri de informații.

Obligațiile de confidențialitate se mențin și după încetarea contractului.

20. Transferul cunoștințelor și continuitatea administrării

Prestatorul va asigura transferul complet al cunoștințelor tehnice către Beneficiar pe durata contractului și la încetarea acestuia.

Prestatorul va asigura:

- documentarea arhitecturii sistemului și a infrastructurii tehnice;
- documentarea procedurilor de instalare, configurare și administrare;
- transmiterea tuturor manualelor și ghidurilor de administrare;
- instruirea personalului desemnat de Beneficiar privind administrarea sistemului;
- furnizarea tuturor informațiilor necesare pentru preluarea administrării sistemului de către Beneficiar sau de către un alt prestator.

La încetarea contractului, Prestatorul va acorda suport pentru transferul ordonat al administrării sistemului, fără întreruperea funcționării serviciilor.

21. Accesul Beneficiarului la infrastructură și cod

Pentru a asigura independența operațională a Beneficiarului și continuitatea serviciilor, Prestatorul va asigura:

- accesul Beneficiarului la codul sursă al sistemului;
- accesul la documentația tehnică completă;
- accesul la configurațiile infrastructurii și aplicației;
- accesul la scripturile de instalare și actualizare;
- accesul la instrumentele de monitorizare și administrare.

Beneficiarul va avea dreptul de a utiliza aceste informații pentru administrarea sistemului sau pentru transferul serviciilor către un alt prestator.

Prestatorul nu va introduce mecanisme tehnice sau contractuale care ar limita accesul Beneficiarului la sistem sau ar crea dependență exclusivă de prestator.

II. Caiet de sarcini

Mentenanța evolutivă, dezvoltarea funcționalităților suplimentare pentru Sistemul Informațional e-Consulat

1. Obiectul achiziției

Prezentul caiet de sarcini stabilește cerințele tehnice și funcționale pentru achiziția serviciilor de dezvoltare și extindere a funcționalităților Sistemului Informațional e-Consulat, utilizat de Ministerul Afacerilor Externe (MAE) și de Misiunile Diplomatice și Oficiile Consulare (MDOC).

Sistemul e-Consulat este utilizat pentru gestionarea activităților consulare și prestarea serviciilor consulare către cetățeni.

Scopul dezvoltărilor este:

- digitalizarea proceselor consulare;
- reducerea utilizării documentelor pe suport de hârtie;
- îmbunătățirea eficienței activității consulare;
- optimizarea raportării și monitorizării activităților consulare.

2. Cadrul normativ aplicabil

Ofertantul trebuie să asigure conformitatea soluției propuse cu cadrul normativ aplicabil sistemelor informaționale guvernamentale.

În mod obligatoriu, sistemul trebuie să respecte cerințele prevăzute de:

- legislația privind protecția datelor cu caracter personal;
- standardele de securitate cibernetică aplicabile sistemelor informaționale;
- standardele de interoperabilitate ale platformelor guvernamentale.

3. Conformarea la Modelul Unitar de Design (MUD)

Toate dezvoltările realizate în cadrul sistemului e-Consulat vor respecta prevederile Modelului Unitar de Design (MUD) aprobat prin Hotărârea Guvernului nr. 677/2025.

În acest sens, dezvoltatorul va asigura:

- alinierea interfeței grafice la standardele MUD;
- utilizarea componentelor și elementelor de design stabilite în ghidul oficial;
- respectarea principiilor de accesibilitate și utilizabilitate;
- compatibilitatea cu ghidurile publicate pe platforma mud.egov.md.

4. Integrarea cu platformele guvernamentale

Sistemul trebuie să permită integrarea cu platformele guvernamentale existente.

În mod obligatoriu, sistemul trebuie să fie compatibil cu:

- MPass – autentificarea utilizatorilor;
- MConnect – schimbul de date între sisteme;
- MPay – procesarea plăților;
- MSign – semnătura electronică.

5. Cerințe funcționale

5.1. Registrul consular electronic

Ofertantul trebuie să dezvolte o rubrică dedicată Registrului consular electronic, care va permite evidența automată a serviciilor consulare prestate.

Funcționalități minime:

- generarea automată a înregistrărilor în registrul consular;
- autocompletarea datelor solicitantului;
- arhivarea electronică a documentelor;
- generarea evidențelor consulare centralizate;
- posibilitatea de monitorizare a activităților consulare.

Soluția trebuie să permită trecerea graduală la un regim paperless.

5.2. Pre-completarea actelor notariale

Sistemul trebuie să permită:

- pre-completarea datelor pentru mandant și reprezentant;
- utilizarea modelelor standardizate de procuri;
- uniformizarea calității actelor notariale.

5.3. Integrarea datelor statistice

Sistemul trebuie să permită extragerea automată a datelor privind serviciile consulare prestate și generarea rapoartelor statistice.

5.4. Optimizarea funcționalităților existente

Ofertantul trebuie să implementeze ajustări ale funcționalităților existente pentru:

- îmbunătățirea performanței sistemului;
- optimizarea fluxurilor operaționale;
- corectarea erorilor identificate.

5.5. Rubrică pentru legislația consulară

Sistemul trebuie să includă o secțiune dedicată legislației consulare și instrucțiunilor interne.

- Funcționalități minime:
- centralizarea actelor normative;
- actualizarea automată a linkurilor către sursele oficiale.

5.6. Configurarea serviciilor consulare per MDOC

Sistemul trebuie să permită configurarea individuală a serviciilor consulare pentru fiecare MDOC.

Funcționalități minime:

- activarea sau dezactivarea serviciilor consulare;
- configurarea condițiilor de prestare a serviciilor;
- jurnalizarea modificărilor.

5.7. Personalizarea taxelor consulare

Sistemul trebuie să permită configurarea taxelor consulare la nivel de MDOC.

Funcționalități minime:

- asocierea taxelor cu serviciile consulare;
- configurarea monedei de încasare;
- definirea cursurilor valutare.

6. Cerințe de securitate

Ofertantul trebuie să asigure:

- criptarea comunicațiilor;
- jurnalizarea activităților utilizatorilor;
- jurnalizarea activităților administrative;
- protecția împotriva accesului neautorizat;
- auditarea logurilor.

7. Documentația tehnică

- Ofertantul trebuie să furnizeze:
- arhitectura sistemului;
- documentația tehnică;
- ghidul de instalare;
- ghidul de administrare;
- manualele utilizatorilor.

8. Livrabile

Prestatorul trebuie să livreze:

- codul sursă al funcționalităților dezvoltate;
- documentația tehnică;
- documentația de instalare;
- raportul de testare;
- documentația de acceptanță.

III. Descriere Tehnică – Sistemul Informațional e-Consulat

1. Arhitectura aplicației

Sistemul e-Consulat este construit pe o arhitectură modulară, bazată pe .NET, cu separarea clară a componentelor BackOffice și FrontOffice:

- Layer CrossConcern – conține componente comune, enum-uri și logica reutilizabilă.
- Domain Layer – modele de date și logica centrală a aplicației.
- Database Layer – configurarea și migrarea schemelor SQL.
- Infrastructure Layer – implementări de integrare cu sisteme externe (MPay, MPass, MSign, MNotify, MDelivery etc.).
- Application Layer – logica de business partajată, handler-e pentru FrontOffice și BackOffice.
- FrontOffice și BackOffice Clients – interfețele utilizator și controller-ele API corespunzătoare.

Aplicația expune API-uri RESTful, documentate prin Swagger, care permit interacțiunea între front-end și back-end și integrarea cu servicii externe.

2. Bazele de date utilizate

Sistemul utilizează Microsoft SQL Server+ ca SGBD.

- Entity Framework Core este folosit pentru maparea obiect-relațională.
- Migrațiile de schemă și seed-urile sunt gestionate prin EF Migrations.
- Conexiunile la baze de date sunt configurate în appsettings.json și adaptate pentru medii de dezvoltare, testare și producție.

3. Componente software

Principalele tehnologii și librării folosite:

- Backend: .NET, ASP.NET Core, MediatR, LazyCache, Hangfire (job scheduling), Mapster (object mapping).
- Frontend: Blazor WebAssembly + MudBlazor (UI Material Design), Fluxor (state management), TinyMCE (editor text).
- Integrare API: NSwag pentru generarea clientului API pe baza OpenAPI.

- Depozitare fișiere: MinIO S3-compatible object storage.
- Logging & Observabilitate: Sentry pentru monitorizare și raportare erori.
- Securitate: autentificare prin MPass SAML, semnătura electronică prin MSign, certificate SSL instalate pe server.

4. Componente hardware

- Server aplicație: Windows Server sau Linux (Ubuntu), resurse scalabile în funcție de trafic.
- Server baze de date: SQL Server dedicat sau instanță partajată în mediu securizat.
- Load Balancing și TLS: NGINX/Apache pentru terminarea TLS, WAF și rate limiting.

5. Integrarea cu alte sisteme

e-Consulat se integrează cu:

- MConnect (event streaming) – notificări în timp real.
- MPass – autentificare SAML.
- MSign – semnătura electronică a documentelor.
- MPay – procesarea plăților online (SOAP API).
- MNotify – transmiterea notificărilor.
- MDelivery – livrarea electronică a documentelor.
- E-Appointment – gestionarea programărilor online.

Toate integrările folosesc conexiuni HTTPS și certificate digitale pentru securizarea traficului.

6. Platforma de găzduire

Sistemul este pregătit pentru găzduire hibridă (on-premise sau cloud). Configurațiile pot fi implementate în:

- Azure DevOps pentru CI/CD.
- Containere Docker pentru rularea aplicației în medii orchestrate (opțional).
- SSL/TLS pentru toate endpoint-urile.

7. Tehnologii folosite

Zonă	Tehnologii / Framework-uri
Limbaj programare	C# (.NET)
Frontend	Blazor WebAssembly, MudBlazor, Fluxor
Backend	ASP.NET Core, MediatR, Hangfire
ORM	Entity Framework Core

Baze de date	Microsoft SQL Server
API management	Swagger / NSwag
CI/CD	Azure DevOps
Logging	Sentry, MLog
Stocare fișiere	MinIO (S3-compatible)
Integrare	MPay, MPass, MSign, MNotify, MDelivery

8. Categoriile de specialiști pentru mentenanță

8.1. Administrare sisteme

- Rol: Administrator de sistem / DevOps
- Competențe: Configurare servere Windows/Linux, administrare conturi și drepturi, monitorizare uptime, patch-uri, CI/CD, log management.
- Responsabilități: Menține infrastructura MCloud, coordonează cu STISC, asigură disponibilitate și securitate infrastructură

8.2. Administrare BD

- Rol: Dezvoltator Full-Stack & DBA
- Competențe: C#/ .NET, Blazor, MediatR, EF Core, SQL Server, optimizare interogări, migrații, backup/restore, integrare API (MPass, MPay, MSign).
- Responsabilități: Bug fixing, dezvoltare evolutivă, ajustări legislative, optimizare performanță BD, migrații schemă, restaurare în caz de incident

8.3. Securitate cibernetică

- Rol: Specialist securitate
- Competențe: OWASP, testare penetrare, WAF, audit securitate, răspuns la incidente.
- Responsabilități: Audit periodic, remediere vulnerabilități, aplicare patch-uri critice

8.4. Suport tehnic utilizatori

- Rol: Helpdesk L1/L2
- Competențe: ITIL, cunoaștere fluxuri BO/FO, comunicare eficientă.
- Responsabilități: Preluare tichete, suport utilizatori, escaladare către dezvoltator sau admin sistem