

Specificații tehnice (F4.1)

[Acest tabel va fi completat de către ofertant în coloana 4, iar de către autoritatea contractantă – în coloanele 1, 2, 3, 5]

Numărul procedurii de achiziție: ocds-b3wdp1-MD-1601538386427 din 01.10.2020
Denumirea licitației: Servicii de dezvoltare a SIA "Urmărire penală: E-Dosar"

Cod CPV	Denumirea serviciilor	Specificarea tehnică deplină solicitată de către autoritatea contractantă	Specificarea tehnică deplină propusă de către ofertant	Standarde de referință
1	2	3	4	5
	Servicii			
7221290 0-8	Servicii de dezvoltare a SIA "Urmărire penală: E-Dosar"	Cerințe funcționale a SIA "Urmărire penală: E-Dosar": - Migrarea SIA "Urmărire penală: E-Dosar" pe una din bazele de tip Enterprise MS SQL, Oracle, PostgreSQL cu opțiunile disponibile de clusterizare, care nu presupune un cost de licență sau costul de licență va fi inclus în oferta ca poziție separată; - Crearea unei baze de date noi optimizată pentru citire și exportul în arhivă;	Cerinte functionale: - Pentru realizarea proiectului se va utiliza un sistem de gestiune a bazei de date de tip enterprise (PostgreSQL) deoarece detine toate optiunile de clusterizare necesare si nu necesita un cost de licenta, spre deosebire de MS SQL si Oracle , My SQL.	

		- Configurarea unui proces/flux de restabilire a dosarelor din arhivă, pentru consultare, sau reluarea urmăririi penale; - Ajustarea fluxurilor curente prin exportul automat a dosarului și tuturor documentelor aferente; - Exportul log-urilor (evenimentele jurnalizate) mai vechi de un an în arhivă; - Integrarea cu sistemele terțe relevante SIA RSUD (Registrul de stat al unităților de drept), SIA RSP (Registrul de stat al populației), SIA RST (Registrul de stat al transporturilor), SIA ECCRPP (Sistemul informatic de evidență a cauzelor contravențiilor, amenzilor și a persoanelor care le-au desfășurat), SIA IGPF (Sistemul informațional al Departamentului Poliție de Frontieră), etc., prin intermediul MConect; - Integrarea cu serviciile MPass/MSign/MNotify/ MLog, cu posibilitatea prelungirii certificatelor de tip server pentru utilizarea MPass/MSign; - Adăugarea certificatelor de tip server pentru criptarea traficului browser-server. - Reconfigurarea de pe HTTP pe HTTPS; - Automatizarea infrastructurii pe o scalare orizontală prin containerizarea sistemului SIA "Urmărire penală: E-Dosar" cu posibilitatea utilizării soluției de orchestrare a containerelor (Kubernetes);	- Va fi analizată performanța actuală a sistemului și în funcție de rezultatul analizei se va crea o nouă bază de date astfel încât să răspundă unor indicatorilor desirabili privind performanța. - Configurarea procesului/fluxului de restabilire a dosarelor din arhivă pentru consultare sau reluarea urmăririi penale, precum și ajustarea fluxurilor curente pentru realizarea exportului automat a dosarelor și documentelor aferente, se vor realiza după faza de analiză din cadrul proiectului. - - În cadrul proiectului se va face migrarea datelor din vechea bază de date și/sau se va analiza opțiunea de interoperabilitate a bazelor de date. - Integrarea cu sistemele terțe solicitate (RSP, RSUD, RST, ECCRPP, IGPF) se va realiza prin intermediul platformei de interoperabilitate MConnect după furnizarea de către Procuratura a informației necesare către Agenția Guvernare Electronică și acordarea de către aceasta a accesului aferent. - Integrarea cu serviciile M (Pass, Sign, Notify, Log) se va realiza prin	
--	--	--	--	--

	- Configurarea formularelor tipizate prin intermediul instrumentelor grafice care sunt prevăzute în SIA "Urmărire penală: E-Dosar", cu opțiunea de configurare a formularelor de documente (șabloane) di interfața grafică; - Crearea bazei de date externe pentru arhivă și migrarea tuturor dosarelor cu o soluție finală în această bază; - Exportul evenimentelor mai vechi de 1 an sau 6 luni într-un sistem extern/bază de date specializată pentru monitorizarea și analiza evenimentelor (log monitoring analysis tools); - Crearea unei baze de date suplimentare pentru informația analitică (data warehouse/analytics platform), sau crearea unor tabele separate în baza de date de „arhivă” și reconfigurarea rapoartelor statistice; - Configurarea proceselor resurse umane și transferul automatizat al drepturilor de vizualizare/accesare a dosarelor de transfer, detașare, delegare a angajaților în altă subdiviziune, promovare în funcție sau retrogradare, etc. Cerințe non-funcționale a SIA "Urmărire penală: E-Dosar": - Aplicarea în medii containerizate a diferitor componente ale sistemului de operare,	intemediul web serviciilor impreuna cu reprezentantii EGA si Procuratura. - Pentru criptarea traficului browser-server se vor implementa certificatele de tip server. Sistemul va fi reconfigurat astfel incat sa utilizeze certificate https. - Automatizarea infrastructurii se va realiza prin containerizarea sistemului utilizand tehnologiile docker si Kubernetes si practicile DevOps. Experienta si expertiza in utilizarea acestei stive tehnologice este descrisa in ultimul capitol. - Vor fi configurate in jur de 30 de formulare tipizate utilizand instrumentele grafice ale sistemului Simbase sau programarea acestora utilizand limbajul Php si/sau unul din Framework-urile aferente. - Prin crearea unei baze de date externe intelegem ca pentru a fluidiza activitatea cu dosarele este nevoie de divizarea fluxurilor dosarelor curente de cele finalizate. Astfel, se va crea o componenta separata de arhiva pasiva in care vor fi exportate dosarele finalizate. Ele vor fi disponibila la cautare, desi timpul va fi mai mic decat in cazul dosarelor curente.	
--	---	--	--

		<i>middleware, baze de date, etc.</i>, cu utilizarea tehnologiilor informaţionale de ultima generaţie. - Includerea în ofertă a informaţiei detaliate privind platforma tehnologică recomandată ținând cont de necesitățile Procuraturii stabilite în acest caiet de sarcini. Cerințe de interoperabilitate cu alte sisteme informatice: - Interfețele, fluxurile de mesaje expuse în SIA "Urmărire penală: E-Dosar", trebuie să fie bazate pe standarde deschise. - Interacționarea interfețelor din SIA "Urmărire penală: E-Dosar" cu alte aplicații externe atât în regim real, cat și în regim off-line. - Integrarea mecanismelor bidirecționale de integrare prin API bine structurate, securizate și documentate. - Posibilitatea generării de documente noi, schimb de informații între subdiviziunile Procuraturii, etc. cu accesarea tuturor funcțiilor ale sistemului. - Interfețe standard pentru exportul datelor în cadrul instrumentelor de tipul <i>Data Warehouse</i>.	- Pentru înregistrarea, monitorizarea si analiza evenimentelor se va utiliza suita de aplicatii ELK (Elasticsearch, Logstash, Kibana), https://www.elastic.co/what-is/elk-stack. Exportul evenimentelor mai vechi de 1 an sau 6 luni vor fi exportate intr-un sistem separat pentru a fi analizate. Evenimentele crtice vor fi exportate in serviciul Mlog. - Va fi reevaluată functionalitatea de raportare statistica si se va analiza optiunea de crearea a unei componente separate de tip data warehouse pentru stocarea datelor. - Vor fi configurate urmatoarele procese de resurse umane: transferul automatizat al drepturilor de vizualizare/accesare a dosarelor de transfer, detaşare, delegare a angajaţilor în altă subdiviziune, promovare în funcție sau retrogradare. Cerinte non-functionale - Toate componentele sistemului vor fi containerizate. Stiva docker si Kubernetes sunt nume de referinta in domeniu.	
--	--	--	--	--

		Cerințe de performanță a SIA "Urmărire penală: E-Dosar": - Timpul de răspuns la o solicitare utilizator/serviciu extern nu trebuie să depășească o secundă. - Gestionarea 1000 de sesiuni concurente (conexiuni utilizatori autorizați și sisteme externe). - Includerea în ghidurile de administrare și operare a sistemului informație privind procesele ce pot diminua performanța SIA "Urmărire penală: E-Dosar" și recomandările sale privind rularea concurentă a acestor procese (<i>exemplu: nu se recomandă rularea procesului X de generare a rapoartelor zilnice, simultan cu procesul Y de generare a copiei de rezervă</i>). - Generarea rapoartelor și accesarea informației în scopul analizei fără afectarea performanței operaționale a sistemului la nivel de procesare. - În documentația sistemului vor fi identificate rapoartele cu impact semnificativ asupra performanței și formulate recomandările furnizorului privind generarea rapoartelor respective astfel încât să nu influențeze indicii de performanță a SIA "Urmărire penală: E-Dosar". - Indicarea în ofertă a valorilor minime garantate pentru caracteristicile de	- Stiva tehnologica propusa: Php (limbaj programare), Simbase (sistem mostenit, Php based), PostgreSQL (sistem gestiune baze de date), docker (container), Kubernetes (orchestrare container), MCloud (cloud), MConnect (Interoperabilitate), Mpass (autentificare), Msign (semnatura electronica). O buna parte din urmatoarele cerinte solicitate sunt generice. Am luat act de toate aceste cerinte si confirmam ca, in eventualitatea castigarii licitatiei, acestea vor fi realizate in deplina masura, dupa o analiza prealabila (in prezent, lipsesc o serie de detalii tehnice). Cerințe mentenanță - Functionalitatile de monitorizare a nivelului de incarcare si functionare vor fi dispobile in suita de aplicatii ELK (Elasticsearch, Logstash, Kibana, https://www.elastic.co/what-is/elk-stack). - Va fi configurat un modul de notificari pentru alertrea privind	
--	--	---	---	--

		performanță ale sistemului, cu referință la platforma tehnologica recomandată. Valorile minime garantate nu vor fi mai mici decât cele minime solicitate. - Deținerea capacității de a procesa cel puțin 100000 de operațiuni pe zi. Cerințe pentru mentenanță a SIA "Urmărire penală: E-Dosar": - Deținerea mecanismelor de monitorizare a nivelului de încărcare și funcționare pentru toate componentele cheie. - Generarea notificări în cazul în care performanța componentelor sale degradează (exemplu: timpul de răspuns la interpelările utilizatorilor depășește 2 secunde). - Ofertantul va enumera mijloacele ce vor fi utilizate la depanarea tehnică a sistemului. - Elaborarea mecanismelor de către ofertant, care ar facilita funcțiile de administrare a sistemului cum ar fi: pornirea, resetarea, crearea copiei de rezervă a bazei de date și fișierelor de conținut, restaurarea funcționalității sistemului în baza copiei de rezervă, arhivare date istorice, pregătire date pentru rapoarte complexe, etc.) - Posibilitatea implementării noilor versiuni livrate de furnizor fără a afecta configurările și componentele existente a arhitecturii SIA	perturbarea proceselor critice. Canalul de notificare se va agrea in cadrul proiectului). - Masuri si instrumente pentru un serviciu de depanare eficient: persoane repsonsabile dedicate din partea ambelor echipe, un SLA (service level agreement) agreat, sistem de gestiune incidente (recomandam GitLab service desk). - Facilitarea functiilor de administrare a sistemului vor fi realizate numai dupa o analiza prealabila a procesului curente pentru propunerea unor masuri optime. - Posibilitatea implementarii unmor noi verisuni va fi analizata in contextul in care sistemul actual Simbase detine o astfel de verisune si numai daca este fezabila o astfel de optiune. - Recomdam crearea unei platfrome de teste, avand o configuratie echivalent a cu mediul de productie, pentru testrea noilor functionalitati dezvoltate. Cerințe de scalabilitate - Scalarea sistemului se va produce automat dupa scenarii predefinite	
--	--	--	--	--

		"Urmărire penală: E-Dosar", pentru interacțiunea cu sisteme informatice externe și interne ale Procuraturii. - Posibilitatea de testare și dezvoltare a SIA "Urmărire penală: E-Dosar" în vederea asigurării proceselor solicitate. - Înregistrarea erorilor și excepțiilor în funcționarea sistemului nominalizat cu expunerea utilizatorilor în timpul de lucru cu SIA "Urmărire penală: E-Dosar", clar și explicit. - Posibilitatea prelucrării a tuturor erorilor generate cu înregistrarea și posibilitatea analizei. Cerințe de scalabilitate a SIA "Urmărire penală: E-Dosar": - Configurarea sistemului pentru scalare automată la nivelul componentelor cheie (lag sensitive), atât pe verticală, cât și pe orizontală, fără a întrerupe funcționarea capacității de procesare: adăugarea automata de noi containere și efectuare balansare a încărcării. Cerințe pentru asigurarea securității SIA "Urmărire penală: E-Dosar": - Ofertantul va asigura securizarea sistemului conform politicii de securitate aprobate de către Procuratura Generală.	dupa containerizarea acestuia si configurarea aplicatiei de orchestrare Kubernetes. Cerințe pentru asigurarea securității - Accesul in sistemul e-Case se va realiza in functie de rolurile specifice (granulare) detinute de fiecare utilizator si/sau categorie de utilizator in parte. - Autentificarea in sistem se va realiza prin serviciul MPass Cerințe față de mecanismul de autorizare sistem - Cerintele prezentui capitol vor fi realizate numai dupa o analiza prealabila a sistemului Simbase. Presupunem ca ele exista si este nevoie de configurarea lor. Cerințe față de mecanismul de validare a datelor de intrare/ieșire - Am luat act de cerintele prezentului capitol. Ele vor putea fi realizate numai dupa analiza sistemului curent Simbase si a contextului in care ele sunt solicitate.	
--	--	--	--	--

		- Posibilitatea accesării funcțiilor sale doar după autentificarea cu succes a utilizatorului/administratorului. - Ofertantul va oferi suport sistemului pentru cel puțin următoarele metode de autentificare: în bază de ID și parolă cu dublu factor de autentificare, M-Pass în calitate de mecanism de autentificare a utilizatorilor prin intermediul certificatului digital sau identității mobile. - Înregistrarea utilizatorilor și a informației de profil aferentă acestora: ID, parola, nume, prenume, Email etc.. - Parolele utilizatorilor trebuie să fie protejate. Metoda de protejare a parolelor trebuie să asigure imposibilitatea interceptării, deducerii sau recuperării acestora. - Definirea și implementarea seturilor de politici de utilizare a parolelor. Politicile trebuie să permită setarea cerințelor cel puțin pentru: complexitatea parolei; obligativitatea schimbării parolei; durata de viață a parolei; utilizarea repetată a parolelor; numărul de încercări de autentificare eșuată; dicționar de parole interzise. - Sistemul informatic va furniza utilizatorului în timp util informație cu privire la aplicarea politicilor de utilizare a parolelor (exemplu: mesaj de expirare a parolei în n zile). - Aplicarea diferențiată a politicilor de utilizare a parolelor pentru diferite grupuri de utilizatori.	Cerințe față de mecanismul de jurnalizare și audit - Toate cerințele prezentului capitol vor fi realizate prin suita de aplicații specializate ELK (Elasticsearch, Logstash, Kibana) - Evenimentele critice pot fi exportate automatizat în serviciul Mlog. Cerințe față de mecanismul de gestiune a excepțiilor și erorilor - Am aluat act de aceste cerințe pe care le consideram ca fiind absolut firești pentru un sistem de tipul e-Case. După o analiză a sistemului curent aceste cerințe vor fi realizate în deplină măsură. Cerințe de reziliență și continuitate - Vor fi realizate funcționalitățile de executare a procedurilor de generare automată a copiilor de rezervă și gestiune a copiilor de rezervă istorice. - Vor fi asigurate mecanismele de asigurare a integrității datelor în cazul caderilor la nivelul oricărui componente, restabilire operativă a disponibilității și accesibilității în cazul	
--	--	--	---	--

		- Blocarea, dezactivarea sau suspendarea conturilor utilizatorilor la nivel de aplicație. - Integrarea cu servicii externe de tipul „ISP” (<i>Identity Services Providers</i>). Metodele de autentificare ce trebuie să fie susținute cu implicarea unui ISP extern sunt: ID și parola cu dublu factor de autentificare; Certificate X.509. - Aplicarea diferențiată a metodelor de autentificare, în funcție de resursele accesate. - Setarea numărului de conexiuni simultane ce pot fi inițiate de un utilizator. - Setarea timpului de expirare a sesiunilor utilizatorilor în caz de inactivitate. - Elaborarea mecanismelor eficiente de prevenire a preluării neautorizate a sesiunilor active inițiate de utilizatorii legitimi. - Sesiunea de lucru în SIA ”Urmărire penală: E-Dosar” va fi blocată la solicitarea utilizatorului sau automat, la expirarea sesiunii utilizatorului. Cerințe față de mecanismul de autorizare în SIA ”Urmărire penală: E-Dosar”: - Posibilitatea gestiunii granulare a drepturilor de acces la toate obiectele sistemului informatic și acțiunile posibile asupra acestora: entități, proprietăți ale entităților, formulare electronice, meniuri, rapoarte, acțiuni de creare/vizualizare/actualizare/ eliminare. - Definirea de grupuri de utilizatori și roluri în cadrul sistemului și asocierea utilizatorilor la aceste grupe și roluri.	unor incidente de continuitate, asigurarea a integritatii datelor în cazul unor caderi accidentale la nivelul oricaror componente ale sale. - O eventuala rearhitecturare a sistemului poate fi deciza numai in urma analizei arhitecturii curente si a fezabilitatii acestui proces. Acerst lucru va fi analizat in cadrul proiectului.	
--	--	--	---	--

		- Acordarea drepturilor de acces la nivel de utilizator explicit, grup și rol. Un grup de utilizatori va putea conține mai multe subgrupuri/roluri. Un utilizator poate fi asociat unuia sau mai multor grupuri și roluri, drepturile sale de acces fiind determinate cumulativ. - Acordarea drepturilor de acces bazate pe reguli de procese: modificarea documentului, stare, context dacă utilizatorul este autor sau dacă operațiunea se face într-un anumit interval de timp - Permișiunea atribuirii temporare a drepturilor deținute de un utilizator, către un alt utilizator. Atribuirea va putea fi efectuată cu păstrarea sau suspendarea drepturilor deținute de utilizatorul către care se deleagă drepturile. - Permișiunea ștergerii activităților administrative de către administrator. - Furnizarea vizualizării și rapoarte privind drepturile de acces configurate. Acestea vor putea fi parametrizate în funcție de cel puțin următoarele criterii: grup de utilizatori/rol în, ID utilizator, entitate de business, proprietate aferentă entității de business, acțiuni admise. Cerințe față de mecanismul de validare a datelor de intrare/ieșire: - Deținerea mecanismelor pentru a preveni manipularea datelor de intrare (date de intrare		
--	--	---	--	--

		parvenite de la utilizatorii autorizați, date de intrare parvenite de la aplicații externe) atât la nivel de aplicație cât și la nivel de bază de date. - Acțiunile de modificare a datelor critice și sensibile în cadrul sistemului, vor fi efectuate prin intermediul formularelor, conform fluxului de lucru stabilit pentru aceste date critice. - Efectuarea validării complete și independente a datelor pe partea de nivelul de prezentare, logicii, nivelul de date, în scopul asigurării integrității, completitudinii și corectitudinii datelor. - Datele confidențiale nu vor fi stocate și accesate nesecurizat în fișiere log, caching, etc. - Deținerea mecanismelor de protejare adițională a datelor confidențiale (exemplu: afișarea mascată a datelor, stocarea datelor în formă criptată, autentificarea repetată a utilizatorului etc.). - Deținerea proceduri de rutină pentru verificarea și detectarea posibilelor coruperi a relațiilor de integritate a datelor, mecanisme adecvate pentru a preveni manipularea datelor stocate. Cerințe față de mecanismul de jurnalizare și audit a SIA "Urmărire penală: E-Dosar": - Deținerea componentelor de audit care vor colecta și gestiona centralizat înregistrările de audit la nivelul fiecărui modul al sistemului informatic.		
--	--	---	--	--

		- Componenta de audit va permite configurarea granulară a politicilor de audit. - Posibilitatea stabilirii politicilor de audit la nivel de obiect/entitate/eveniment jurnalizat. - Stabilirea caracteristicilor specifice evenimentelor ce trebuie să fie jurnalizate (exemplu: produse într-un anumit interval de timp, o anumita valoare a proprietarii entității de business). - Fiecare înregistrare de audit va conține cel puțin: momentul în timp al producerii evenimentului; subiectul evenimentului (ID utilizator); obiectul sau entitatea afectată; evenimentul produs; adresa IP a sursei ce a inițiat evenimentul. - Înregistrările de audit nu vor conține informație de proces confidențială. - Jurnalizarea erorilor de audit nu trebuie să afecteze funcționarea normală a sistemului. - Componenta de audit va utiliza ceasul de sistem setat la nivelul sistemului de operare în care rulează componenta de audit. - Componenta de audit va deține un mecanism de arhivare a înregistrărilor de audit istorice. Procesul de arhivare va conține: frecvența, vechime date, format arhivare, destinație etc.). - Generarea automată a notificări către persoanele responsabile la producerea anumitor evenimente de securitate, conform configurațiilor setate.		
--	--	--	--	--

		- Componenta de audit va putea fi integrată în baza standardelor deschise cu soluții de tipul SIEM (<i>Security Incident and Event Management</i>) în vederea preluării înregistrărilor de audit produse în cadrul sistemului, de către soluțiile respective. - Fixarea versiunilor istorice ale datelor, ce vor fi considerate deosebit de sensibile. - Activitățile de schimbare stări și responsabili înregistrări vor fi jurnalizate. - Elaborarea mecanismelor pentru accesarea și procesarea evenimentelor jurnalizate, inclusiv filtrarea înregistrărilor de audit după orice câmp deținut și exportul acestora în format uzual. Instrumentele de audit ale sistemului vor putea fi utilizate și în scopul importului arhivelor cu fișiere de audit pentru activități de analiza ocazionale. - Posibilitatea jurnalizării evenimentelor de proces în paralel și sincron prin intermediul sistemului guvernamental de jurnalizare <i>MLog</i>, mecanisme de configurare a evenimentelor de proces care vor fi jurnalizate alternativ și prin intermediul serviciului <i>MLog</i>. Cerințe față de mecanismul de gestiune a excepțiilor și erorilor: - Înregistrarea centralizată la toate excepțiile și erorile generate de componentele sale. - La producerea unei erori, SIA "Urmărire penală: E-Dosar" va afișa utilizatorului un		
--	--	---	--	--

		mesaj de eroare generic. Acesta poate conține un cod de eroare și un identificator unic al erorii, pentru a facilita implicarea serviciilor de suport. - Toate erorile care vor expune utilizatorilor în timpul de lucru cu SIA "Urmărire penală: E-Dosar" vor fi suficient de clare și sugestive. - Deținerea instrumentelor necesare pentru analiza și procesarea înregistrărilor aferente excepțiilor și erorilor. - Generarea automată a notificărilor către persoanele responsabile la producerea anumitor erori în funcționarea a componentelor sale. Cerințe de reziliență și continuitate a SIA "Urmărire penală: E-Dosar": - Implementarea instrumentelor pentru executarea procedurilor de generare automată a copiilor de rezervă și gestiune a copiilor de rezervă istorice. - Deținerea mecanismelor de asigurare a integrității datelor în cazul căderilor la nivelul oricăror componente, restabilirea operativă a disponibilității și accesibilității în cazul unor incidente de continuitate, asigurarea a integrității datelor în cazul unor căderi accidentale la nivelul oricăror componente ale sale. - Arhitectura SIA "Urmărire penală: E-Dosar" trebuie să fie rezistentă la căderi de		
--	--	---	--	--

		componente și să nu dețină puncte singulare de cădere (SPOF). Cerințe fata ofertant: - Capacitatea organizațională și resurse umane (nr. specialiștilor TI angajați min. 15 persoane); - Experiență de minim 7 ani în dezvoltarea sistemelor informatice - Reputația profesională a organizației și a echipei, minim 5 scrisori de recomandare sau referințe de la beneficiari privind implementarea de sisteme informatice complexe; - Proiecte de complexitate similare în sectorul public din Republica Moldova, cu prezentarea descrierilor activităților specifice, cu accent pe migrarea datelor (minim 2 proiecte); integrarea cu serviciile de platforma e-Gov (minim 2 proiecte); interoperabilitatea cu sistemele terțe enumerate prin intermediul MConnect (minim 2 proiecte); containerizarea și orchestrarea sistemelor prin intermediul docker și Kubernetes (minim 2 proiecte). - Experiența în elaborarea și implementarea soluțiilor bazate pe PHP, PostgreSQL, MS SQL, My SQL, docker, Kubernetes. - Copiile certificatelor: ISO 9001:2015; ISO 20000-1:2018; ISO 27001:2013; ISO 37001:2016;	Cerințe fata ofertant: - Asocierea are la dispozitie in jur de 40 de specialisti IT (PM, ingineri software, specialisti Cloud si DevOps, ingineri infrastructura). - Membrii asocierii au, fiecare in parte, mai mult de 10 ani experienta in furnizarea solutiilor IT cu accent pe dezvoltarea sistemelor informatice (Esempla Systems) si serviciilor de cloud si infrastructura (BTS Pro). - Reputatia profesionala a organizatiilor poate fi dovedita inclusiv prin scrisorile de recomandare de la urmatoarele autoritati publice contractante: (Ministerul Justitie / Sistem de inregistrarea a garantiilor mobile; Ministerul Justitiei / Sistem e-Apostila; STISC / Sistem de gestiune incidente IT; Autoritatea Nationala de Integritate / Sistem e-Integritate; Consiliul pentru prevenirea si eliminarea discriminarii si asigurarea egalitate / Sistem e-Case. Scrisorile sunt anexate la prezenta oferta. - Proiecte de complexitate similara: Migraare date: Proiect SIARG, Ministerul justitiei (migrarea datelor din vechiul sistem al gajurilor (baza	
--	--	---	---	--

		- Certificat de conformitate al Sistemului de management al serviciilor în domeniul tehnologiei informației ISO/IEC 20000-1:2011 (sau similar) – copie – confirmată prin semnătură și ștampilă; - Manager de Proiect, certificat PMI. - Arhitect de sistem, min. 5 ani experiență, certificate în domeniul cloud, CV atașat cu descrierea activităților conform CPI.4. - Inginer-programator x 2, min. 5 ani experiență în utilizarea tehnologiile specificate CPI.5. - Inginer Devops, min. 2 ani experiență în utilizarea tehnologiilor docker, Kubernetes.	de date Informix, peste 1 milion înregistrări) în noul sistem (baza de date PostgreSQL); Proiect e-Integritate (migrarea datelor existente (cca. 500 mii declaratii) în sistemul e-Integritate, migrare din MS SQL în PostgreSQL); Proiect Arhiva Chisinau Gaz (migrare cca. 3 milioane de înregistrări în noul sistem de arhivă digitală, migrare din MS SQL și Oracle în PostgreSQL). Integrare cu serviciile eGov: MCabinet, MSign, MPass, MLog (proiect MNotify, AGE); MCabinet, MSign, MPass, MLog (Proiect MPower, AGE); MPass, MSign, MLog, MPay (Proiect e-Apostila, Ministerul Justiției); Mpay, MSign (Apa Canal Chisinau); MPass, MSign, MPay, MLog (IMSERV, BMA). Interoperabilitate MConnect: Registrul de stat al populației (RSP), Registrul de stat al unitatilor de drept (RSUD), sistem de monitorizare contravenții, amenzi și contravenienți (ECCRPP, MAI), sistem monitorizare traversări frontiere (MAI, Pol. Frontiera); sistem de management vize (SIGV, MAIE);	
--	--	---	--	--

			sisteme mostenite de documentare persoane (BMA); sisteme periferice pentru citirea si captura datrelor biometrice si pasapoarte (Speed identity G3, 3M (Proiect IMSERV, BMA); RSP, RSUD, Cadastru, Politia frontiera, Serviciul fiscal de stat SFS (Proiect e-Integritate, ANI); RSP, RSUD, Registrul de stat transporturi / RST (Proiect SIARG, Ministerul Justitiei); RSP, RSUD, SFS, Trezorerie (Proiect MTender, Ministerul finantelor); Containerizare si orchestrare: Proiectele MPower si MNotify, AGE (toate componentele sistemelor containerizate utilizand docker, iar orchestrarea realizata prin Kubernetes; Proiect MTender, Ministerul finantelor (platforma e-Licitatia containerizata (docker), orchestrare (Kubernetes); componenta de interoperabilitate cu MConnect containerizata (docker). - Experiența în elaborarea și implementarea soluțiilor bazate pe PHP, PostgreSQL, MS SQL, My SQL, docker, Kubernetes. Stiva tehnologica solicitata in prezentul caiet de sarcini a fost	
--	--	--	--	--

			utilizata in urmatoarele proiecte: e-Integritate, sistem de inregistrare si gestiune a declaratiilor de avere si interese personale. Beneficiar ANI. Tehnologii utilizate: PHP, PostgreSQL; SIARG, sistem pentru inregistrarea si gestiunea garantiilor mobile. Beneficiar Ministerul Justitiei. Tehnologii utilizate: PHP, PostgreSQL; e-Apostila, sistem de inregistrare si emitere a apostilelor electronice. Beneficiar Ministerul Justitiei. Tehnologii utilizate: PHP, PostgreSQL; MTender, e-Licitatie, sistem de achizitii online. Beneficiar Ministerul Finantelor. Tehnologii utilizate: PHP, PostgreSQL, docker, Kubernetes; MNotify, sistem de notificari. Beneficiar Agentia Guvernare Electronica. Tehnologii utilizate: MS SQL, docker, Kubernetes; MPower, sistem de emitere si gestiune autorizari. Beneficiar Agentia Guvernare Electronica. Tehnologii utilizate: MS SQL, docker, Kubernetes; Revizia.md, aplicatie de scoring. Beneficiar AGER. Tehnologii utilizate: php, PostgreSQL, docker. - Certificare ISO. Asocierea detine urmatoarele certificate: ISO 9001:2015; ISO 27001:2013	
--	--	--	---	--

			(Esempla) si ISO 9001:2015; ISO 27001:2013; ISO 14001:2015; SM SR EN ISO/IEC 20000-1:2018; ISO 37001:2016 (BTS Pro). Certificatele sunt anexate la prezenta oferta. - Echipa de proiect: Manager de proiect - Tatiana Berlinschi, 10 ani experienta, CV si certificate PMI atasate; Architect de sisteme - Dumitru Virtosu, 10 ani experienta, CV si certificari cloud atasate (AWS Solution architect, AWS SysOps, certificate atasate); Ingineri software - Sergiu Garaba, 10 ani experienta si Victor Tudor, 7 ani experienta, CV-uri atasate; Specialist DevOps - Alexandr Gorodetchi, 5 ani experienta in administrare sisteme, 2 ani in utilizarea practicilor si instrumentelor DevOps si Kubernetes, CV atasat	
--	--	--	---	--

Semnat: Semnat digital Numele, Prenumele: Dorin Gritcan În calitate de: Reprezentant legal al Asocierii

Ofertantul: Asocierea dintre Esempla Systems-BTS Pro Adresa: str. Bucuriei 1/6, Chisinau, Moldova