MINISTARSTVO PRAVDE
Broj 04-426/25-12329/16
Podgorica, 05.02.2026 god.

14.02.2026

UGOVOR O JAVNOJ NABAVCI

Ovaj ugovor zaključen je između:

Naručioca: Ministarstvo pravde sa sjedištem u Podgorici, ulica Vuka Karadžića br. 3, PIB: 11070094, koga zastupa v.d. sekretara, Đorđije Ivanović, (u daljem tekstu: Naručilac)

i

Ponuđača: "E-lavirint" DOO Podgorica, Ul. Marka Radovića br. 20/30, 81000 Podgorica, PIB: 02706563, Broj žiro računa: 520-9022-92, Naziv banke: Hipotekarna banka AD Podgorica, koga zastupa Aleksandar Mirković, izvršni direktor (u daljem tekstu: Izvršilac).

OSNOV UGOVORA:

Tenderska dokumentacija za otvoreni postupak javne nabavke za nabavku usluga – Nabavka i implementacija PAM (Privileged Access Management) sistema za pristup IKT serverskoj infrastrukturi Ministarstva pravde, broj 04-426/25-12327/3 od 24.11.2025. godine.

Broj i datum Odluke o izboru najpovoljnije ponude 04-426/25-12327/15 od 19.01.2026. godine.

Ponuda Izvršioca **"E-lavirint" DOO Podgorica** broj 149077 od 16.12.2025. godine.

Član 1

Predmet ovog ugovora je nabavka usluge - Nabavka i implementacija PAM (Privileged Access Management) sistema za pristup IKT serverskoj infrastrukturi Ministarstva pravde, prema Tenderskoj dokumentaciji broj: 4-426/25-12327/3 od 24.11.2025. godine, Odluci o izboru najpovoljnije ponude broj: 04-426/25-12327/15 od 19.01.2026. godine i ponudi Izvršioca broj: 149077 od 16.12.2025. godine:

Nabavka i implementacija open-source Privileged Access Management (PAM) sistema koji obezbjeđuje povjerljivost, dostupnost i integritet podataka kroz centralizovano upravljanje privilegovanim nalozima i kontrolu pristupa. Rješenje je predviđeno za do 20 korisnika ali sa mogućnošću proširenja do 1000 korisnika. PAM sistem omogućava bezbjedan pristup, audit i kontrolu svih aktivnosti privilegovanih korisnika, uz potpuni nadzor, snimanje sesija i zaštitu lozinki. 3. Funkcionalni Zahtjevi Rješenje mora podržavati 4A funkcionalnosti: Autentifikaciju, Autorizaciju, Upravljanje nalozima i Reviziju (Audit). PAM mora biti zasnovan na web-arhitekturi i omogućiti pristup sljedećim platformama i protokolima: Linux, Windows, Kubernetes, Database, RemoteApp (SSH, Telnet, RDP, VNC, K8s, MySQL, MariaDB, ClickHouse, DB2, Dameng, PostgreSQL, Oracle, SQL Server, Redis, MongoDB). Rješenje mora onemogućiti otkrivanje lozinki korisnicima, evidentirati sve aktivnosti, blokirati opasne SQL upite i ograničiti prenos datoteka i clipboard pristup. Upravljanje korisnicima, ulogama, i

resursima Sistem mora podržavati vođenje korisničkih naloga (kreiranje, deaktiviranje, brisanje) i prateće grupe korisnika. Sistem mora podržavati definisanje uloga (roles) sa različitim privilegijama (RBAC) kao što su korisnik, administrator, auditor, sl.. Sistem mora podržavati upravljanje resursima ("assets"): mrežni uređaji, serveri, storage uređaji, I ostala serverska infrastruktura, baze podataka, klasteri, RemoteApp-servisi, platfore za virtuelizaciju infrastrukture I sl. Sistem mora podržavati "tagging" i organizovanje resursa u zone / organizacione strukture radi lakšeg grupisanja i primjene politika odnosno kontrola. Sistem mora omogućiti određivanje dozvola korisniku ili grupi, resursu pa nakon toga određivanje vrste pristupa (npr. pristup, upravljanje, pregled). Sistem mora omogućiti da dozvole resursa propagiraju ("kaskadno") sa nadređenih čvorova na podređene. Sistem mora omogućiti audit nad korisničkim ulogama i njihovim promjenama (ko, kada, koja uloga je dodjeljena odnosno uklonjena). Autentifikacija i pristup Sistem mora omogućiti integraciju sa autentifikacionim mehanizmima: LDAP/AD, CAS, OIDC, SAML2, OAuth2, RADIUS. Sistem mora imati mogućnost MFA odnosno 2-faktorsku autentifikacije. Sistem mora omogućiti kontrolu pristupa na osnovu IP adrese, geografske lokacije, vremenskih pravila, pravila prihvatanja, odbijanja, login-pregleda. Sistem mora omogućiti pravila koja ograničavaju na koji način i kada korisnik može pristupiti resursu (npr. dozvoljeni protokoli, vrsta klijenta, vrijeme, IP). Sistem mora omogućiti "command filtering" tokom sesije: blokada/filtriranje naredbi koje korisnik može izvršiti na kranjem sistemu (npr. SSH komande, SQL komande i sl). Sistem mora omogućiti "data masking / output cleansing": mogućnost da se izlaz (npr. baze podataka ili terminal) maskira ili ograniči radi povjerljivosti. Sistem mora podržavati "just-in-time" pristup ili pristup na zahtjev (request/approval workflow) za korisnike kojima pristup mora biti odobren prije nego dobiju pristup resursu. Povezivanje prema resursima i protokolima Sistem mora omogućiti pristup target resursima preko web-pregledača (web terminal): SSH, Telnet, RDP, VNC, Kubernetes, baze podataka, RemoteApp. Sistem treba omogućiti pristup takođe putem desktop klijenata (po mogućnosti), za SSH/SFTP/RDP gdje je korisnički slučaj to zahtijeva. Sistem mora podržavati broj različitih tipova ciljanih sistema: Linux/Unix, Windows, mrežni uređaji (network devices), baze podataka (MySQL, MariaDB, PostgreSQL, MongoDB, Redis, ClickHouse, Dameng, Oracle, SQL Server) i klasteri Kubernetes. Sistem mora omogućiti pregled/odabir kredencijala (računa) za pristup krajnjim sistemima bez da se lozinka otkriva korisniku (npr, korisnik bira iz liste, ali nema mogućnost pregleda lozinke). Sistem mora omogućiti transfer fajlova i clipboard-kontrolu u sesiji (primjer: SFTP web-klijent za prijenos, ograničenje smjera prijenosa, zabrana ako potrebno) Snimanje sesija, revizija i analiza. Sistem mora snimati sve sesije u skladu sa protokolima: oSSH/Telnet: snimanje komandi + timestamp + korisnik odnosno korisnički nalog oRDP/VNC: snimanje video-zapisa (MP4 ili ekvivalent) ekrana sesije. oBaze podataka: snimanje SQL upita i (gdje primjenjivo) rezultata. Sistem mora omogućiti centralizovano skladištenje snimaka i logova u okviru lokalnog filesistema uz mogućnost arhiviranja, hash verifikacije i NTP sinhronizacije. Sistem mora omogućiti playback (reprodukciju) snimljenih sesija sa kontrolama: premotavanje, traženje po vremenu, filtriranje po korisniku odnonso korisničkom nalogu. Sistem mora bilježiti i čuvati audit zapise: korisnički login/logout, promjene autorizacija, file transferi, clipboard aktivnosti, komande, greške, neuspjeli pokušaji pristupa. Sistem mora podržavati REST API interfejs za integraciju sa SIEM, ITSM i IAM sistemima. Logovi i audit podaci moraju biti eksportovani u centralni SIEM sistem putem Syslog/HTTP protokola. Sistem mora omogućiti metapodatke i strukturu logova koja omogućava forenzičku analizu i izveštavanje. Upravljanje privilegovanim nalozima i tajnama. Sistem mora upravljati privilegovanim nalozima ("privileged accounts") i omogućiti da korisnici pristupaju krajnjim sistemima bez vidljive lozinke. Sistem mora podržati automatsku rotaciju lozinki, ključeva (gdje je moguće).

Sistem mora omogućiti sigurnu pohranu kredencijala (enkripciju) i kontrolu pristupa tim kredencijalima. Sistem mora omogućiti reviziju pristupa privilegovanim računima: ko je ostvarion pristup, kada, na koji resurs, za koliko dugo, šta je radio. Automatizacija i integracije Sistem mora omogućiti REST API i/ili CLI za automatsko kreiranje/uklanjanje korisnika, resursa, autorizacija, izvještaja. Sistem mora se integrisati sa IAM sistemima (Identity & Access Management), ITSM (ticketing), i/ili LDAP/AD za sinhronizaciju korisnika i grupa. Sistem mora podržati notificiranje (email/SMS) pri određenim događajima (npr. neuspjeli login) Skalabilnost Sistem mora podržati deployment u HA-clustera (Active-Active ili Active-Standby) za visoku dostupnost. Korisničko iskustvo i upravljanje Sistem mora imati web-interfejs za korisnike (pristup resursima) i za administratore (upravljanje, izvještaji). Sistem mora omogućiti "jedan klik" pristup korisnicima za autorizirane resurse, bez potrebe za ručnim unošenjem lozinke.

Član 2

Rok izvršenja ugovora je 30 dana od dana zaključivanja ugovora.

Mjesto izvršenja ugovora je Ministarstvo pravde.

Član 3

Ukupna vrijednost usluga, prema prihvaćenoj ponudi broj: 149077 od 16.12.2025. godine, iznosi **25.000,00 eura bez uračunatog PDV-a.**
PDV: **5.250,00 €**

Rok plaćanja: 30 dana od dana dostavljanja fakture.

Način plaćanja: Virmanski. Plaćanje će se obaviti nakon potpisivanja Zapisnika o uspješno izvršenoj instalaciji i implementaciji PAM sistema na infrastrukturi Naručioca, koji je potpisan od strane ovlašćenog lica Direktoraat za IKT pravosuđa.

Član 4

Izvršilac se obavezuje:

- da rukovodi izvršenjem svih usluga;
- da obezbijedi kompletnu dokumentaciju po kojoj se izvode usluge;
- da snosi troškove naknade korišćenja patenata i odgovoran je za povredu zaštićenih prava intelektualne svojine trećih lica.

GARANCIJA ZA DOBRO IZVRŠENJE UGOVORA

Član 5

Izvršilac se obavezuje da Naručiocu u trenutku potpisivanja ovog Ugovora preda neopozive, bezuslovne i naplative na prvi poziv garanciju za dobro izvršenje ugovora, za slučaj povrede ugovorenih obaveza u iznosu od 10 % od vrijednosti ugovora.

Garancija za dobro izvršenje ugovora treba da važi sedam dana duže od roka trajanja ugovora.

Navedenu garanciju Naručilac može aktivirati u svakom momentu kada nastupi neki od razloga za raskid ovog Ugovora.

Član 6

Ugovorne strane su saglasne da do raskida ovog Ugovora može doći ako Izvršilac ne bude izvršavao svoje obaveze u rokovima i na način predviđen Ugovorom.
Naručilac je obavezan da u slučaju uočavanja propusta u obavljanju posla pisanim putem pozove Izvršioca i da putem Zapisnika zajednički konstatuju uzrok i obim uočenih propusta.

Kontrole kvaliteta usluge se vrši preko ovlašćenih lica Naručioca, sačinjavanjem i potpisivanjem Izvještaja o realizovanim aktivnostima.

Član 7

Za sve što nije definisano ovim Ugovorom primjenjivaće se odredbe Zakona o obligacionim odnosima.

Član 8

Ukoliko u toku trajanja ovog ugovora dođe do bilo kakvih promjena u nazivu ili drugim statusnim promjenama ugovornih strana, tada će sva prava i obaveze ugovorne strane kod koje dođe do takve promjene, preći na njenog pravnog sljedbenika.

Član 9

Izvršilac se obavezuje da u toku trajanja ovog Ugovora, kao i po isteku istog, ne iznose bilo kakve službene ili povjerljive informacije u vezi ovog Ugovora, poslova i aktivnosti Naručioca, bez prethodne pisane saglasnosti Naručioca.

Član 10

Ugovorne strane su saglasne da eventualne sporove povodom ovog ugovora rješavaju sporazumom. U protivnom, sve sporove koji nastanu u vezi sa ovim Ugovorom rješavaće Privredni sud u Podgorici.

Član 11

Ugovor o javnoj nabavci koji je zaključen uz kršenje antikorupcijskih pravila u skladu sa odredbama člana 38 Zakona o javnim nabavkama, ništav je.

Član 12

Ovaj ugovor je zaključen i potpisan od ovlašćenih zakonskih zastupnika strana ugovora i sačinjen je u 6 (šest) istovjetnih primjeraka, od kojih su 3 (tri) primjerka za NARUČIOCA a 3 (tri) primjerka za IZVRŠIOCA.

NARUČILAC
Đorđije Ivanović,
VD sekretara

IZVRŠILAC
Aleksandar Mirković,
Izvršni direktor