

DRUŽBA ZA AVTOCESTE V REPUBLIKI SLOVENIJI

DARS d.d.

POGLAVJE 2

DODATEK 3 - PROJEKTNA NALOGA

za

Vzpostavitev in vzdrževanje PAM orodja

(int. ev. št. 000127/2026)

I. PROJEKTNA NALOGA

1. PREDMET NAROČILA

Namen uvedbe rešitve je centralizirano, sledljivo in nadzorovano upravljanje privilegiranih dostopov notranjih administratorjev in zunanjih izvajalcev.

Predmet naročila je vzpostavitev in vzdrževanje sistema za upravljanje privilegiranih dostopov (PAM) v virtualnem okolju naročnika. Implementacija PAM mora biti izvedena po načelu »na ključ«. Predmet naročila zajema spodnje postavke:

- Implementacija PAM,
- licence / pravice uporabe za obdobje 36 mesecev,
- podpora in dodatne storitve (504 ur / 36 mesecev),
- osnovno vzdrževanje in odzivnost* in
- morebitne dodatne licence*.

** Postavki »Osnovno vzdrževanje in odzivnost« ter »Morebitne dodatne licence« sta ovrednoteni s strani naročnika in sta fiksni. Postavka »Morebitne dodatne licence« se koristi samo v primeru dejanske potrebe naročnika po dokupu dodatnih licenc v času trajanja pogodbe. Naročnik postavke ni dolžan koristiti.*

2. OSNOVNA IZHODIŠČA IN SISTEMSKO OKOLJE NAROČNIKA

- Rešitev mora biti nameščena in mora delovati v VMware virtualnem okolju naročnika,
- naročnik zagotovi infrastrukturne vire, omrežno povezljivost, certifikate, DNS, NTP, SMTP, SIEM in okolje za varnostno kopiranje,
- strojna oprema in osnovna virtualizacijska infrastruktura nista predmet tega naročila

3. LICENČNE IN KOLIČINSKE ZAHTEVE

- Ponujene licence oziroma pravice uporabe morajo veljati 36 mesecev,
- ponujena rešitev mora licenčno pokrivati 100 ciljnih sistemov,
- ponujena rešitev mora licenčno pokrivati 20 sočasnih uporabnikov,
- če je licenčni model ponujene rešitve vezan na poimenske uporabnike, naročnik kot okvirni, nezavezujoči podatek navaja do 180 poimenskih uporabnikov; zavezujoča količina je 20 sočasnih uporabnikov,
- postavka »Morebitne dodatne licence« je namenjena morebitnemu dokupu licenc v času veljavnosti pogodbe.

4. MINIMALNE TEHNIČNE ZAHTEVE

4.1 PAM rešitev

- Rešitev mora biti namenjena upravljanju privilegiranih dostopov.
- Rešitev mora biti nameščena in mora delovati v virtualnem okolju naročnika.
- Rešitev mora omogočati postavitev v načinu visoke razpoložljivosti. Implementacija visoke razpoložljivosti na ravni aplikacije ni predmet tega naročila; visoko razpoložljivost na ravni infrastrukture zagotavlja naročnik.
- Rešitev mora omogočati integracijo z Microsoft Active Directory in Entra ID imenikom.
- Rešitev mora omogočati uporabo večfaktorske avtentikacije (MFA).
- Rešitev mora omogočati pošiljanje dogodkov v SIEM.
- Rešitev mora omogočati pošiljanje obvestil uporabnikom oziroma skrbnikom po elektronski pošti.
- Rešitev mora omogočati varnostno kopiranje in obnovo konfiguracije oziroma podatkov rešitve.

- Rešitev mora zagotavljati šifriranje občutljivih podatkov, poverilnic, revizijskih zapisov in posnetkov sej v mirovanju in pri prenosu.
- Rešitev mora omogočati uvoz podatkov iz CSV ali drugega strukturiranega zapisa.
- Rešitev mora omogočati integracijo z drugimi sistemi preko dokumentiranega programskega vmesnika, najmanj REST API ali drugega uradno podprtega vmesnika.

4.2 Upravljanje sej

- Rešitev mora omogočati vzpostavljanje sej najmanj po protokolih RDP, SSH, HTTPS/SSL in SFTP/SCP.
- Rešitev mora omogočati dostop do ciljnega sistema brez razkritja gesla ciljnega računa končnemu uporabniku.
- Rešitev mora za standardne protokole omogočati povezovanje brez namestitve dodatnih odjemalcev na ciljne sisteme.
- Rešitev mora omogočati omejevanje dostopa po uporabnikih, skupinah, ciljnih sistemih, časovnih omejitvah in izvornem IP naslovu.
- Rešitev mora omogočati združevanje uporabnikov in ciljnih sistemov v skupine za potrebe dodeljevanja pravic.
- Rešitev mora omogočati dostop do ciljnih sistemov na podlagi zahtevka, ki ga potrdi ena ali več pooblaščenih oseb.
- Rešitev mora omogočati časovno omejitev odobrenega dostopa.
- Rešitev mora omogočati snemanje sej in zbiranje metapodatkov o sejah.
- Rešitev mora omogočati šifriranje posnetkov sej oziroma zaščito posnetkov pred nepooblaščenim dostopom.
- Rešitev mora omogočati nadzor privilegiranih sej v realnem času in prekinitev aktivnih sej.
- Rešitev mora omogočati revizijsko sled dostopov in izvedenih aktivnosti.
- Rešitev mora omogočati zgodovinski pregled dostopov po uporabnikih in ciljnih sistemih.
- Rešitev mora za tekstovne seje omogočati beleženje izvedenih ukazov.
- Rešitev mora omogočati določitev dovoljenih oziroma prepovedanih ukazov za tekstovne seje ali obveščanje ob uporabi tveganih ukazov.
- Rešitev mora omogočati nadzorovano uporabo odložišča in prenosov datotek v okviru privilegiranih sej.
- Rešitev mora omogočati pripravo poročil o dostopih, sejah in uporabniških aktivnostih.

4.3 Upravljanje gesel in skrivnosti

- Rešitev mora omogočati varno hrambo privilegiranih gesel, SSH ključev in drugih skrivnosti.
- Rešitev mora omogočati samodejno rotacijo gesel in SSH ključev za podprte ciljne sisteme.
- Rešitev mora omogočati določitev urnikov rotacije gesel.
- Rešitev mora omogočati določitev izjem od samodejne rotacije gesel oziroma SSH ključev.
- Rešitev mora omogočati nastavitev politik gesel najmanj glede dolžine gesla, uporabe velikih in malih črk, števil, posebnih znakov ter izključitve nedovoljenih znakov in nizov znakov.
- Rešitev mora omogočati nastavitev različnih politik gesel za različne ciljne sisteme oziroma skupine računov.
- Rešitev mora omogočati generiranje gesel z določenim rokom veljavnosti.
- Rešitev mora omogočati generiranje časovno omejenih ali enkratnih gesel oziroma poverilnic.
- Rešitev mora omogočati nadzorovan prikaz oziroma izdajo gesla, kadar je tak način uporabe dovoljen.
- Rešitev mora omogočati upravljanje gesel servisnih računov, kjer je to podprto s strani ciljnega sistema.

4.4 Dostop zunanjih izvajalcev

- Rešitev mora omogočati dostop zunanjih izvajalcev z naročnikovimi AD ter Entra ID uporabniškimi računi.
- Dostop zunanjih izvajalcev mora biti zaščiten z večfaktorsko avtentikacijo (MFA).
- Rešitev mora omogočati časovno omejenost in revizijsko beleženje dostopov zunanjih izvajalcev.
- Rešitev mora omogočati dostop zunanjih izvajalcev samo do odobrenih ciljnih sistemov.
- Rešitev mora omogočati dostop zunanjih izvajalcev preko posredniškega modela oziroma Jump strežnikov.
- Rešitev mora omogočati snemanje sej zunanjih izvajalcev za sisteme, ki jih določi naročnik.

4.5 Hramba, revizija in poročanje

- Rešitev mora hraniti revizijske zapise in posnetke sej najmanj 180 dni.
- Velikost video posnetkov sej ne sme presegati povprečno 3MB na minuto snemanja.
- Dostop do posnetkov sej mora biti omejen na pooblaščen osebe z ustrezno vlogo.
- Vsak ogled, izvoz ali brisanje posnetka seje mora biti zabeležen.
- Rešitev mora omogočati izvoz revizijskih podatkov za nadaljnjo obdelavo.
- Rešitev mora omogočati pripravo poročil najmanj za uporabniške dostope, ciljne sisteme, posnete seje, zahteve, odobritve, neuspele poskuse dostopa in spremembe nastavitve.
- Rešitev mora omogočati časovno žigosanje oziroma časovno sledljivost revizijskih zapisov.

4.6 Uporabniški vmesnik in vloge

- Rešitev mora omogočati uporabo preko spletnega vmesnika.
- Spletni vmesnik mora delovati v aktualnih podprtih različicah brskalnikov Microsoft Edge, Google Chrome in Mozilla Firefox.
- Rešitev mora omogočati ločene vloge oziroma uporabniške profile najmanj za navadne uporabnike, odobritelje dostopov, revizorje in skrbnike rešitve.
- Ne glede na poimenovanje vlog mora biti omogočena ločitev pravic za uporabo ciljnih dostopov, odobritve dostopov, revizijski pregled in (sistemska) administracijo rešitve.
- Rešitev mora omogočati omejevanje dostopa uporabnikov samo na ciljne sisteme, račune in funkcionalnosti, za katere imajo dodeljene pravice.

5. STORITVE IMPLEMENTACIJE

Izvajalec mora zagotoviti vse storitve, potrebne za vzpostavitev rešitve v okolju naročnika. To zajema vsaj:

- analizo okolja in priprava načrta implementacije,
- namestitev in konfiguracijo rešitve,
- integracijo z AD imenikom, Entra ID imenikom, MFA in SIEM,
- vključitev začetnega nabora ciljnih sistemov, ki obsega 30 ciljnih sistemov, ki jih določi naročnik,
- pripravo dokumentiranih postopkov za vključitev nadaljnjih enakovrstnih ciljnih sistemov, ki jih naročnik vključi sam,
- nastavitve snemanja sej, politik dostopa, upravljanja gesel in rotacije gesel,
- testiranje delovanja rešitve,
- pripravo tehnične dokumentacije,
- izobraževanje skrbnikov sistema.

6. VZDRŽEVANJE, PODPORA IN ODZIVNOST

6.1 Osnovno vzdrževanje in odzivnost

Osnovno vzdrževanje in odzivnost sta zajeta v fiksni mesečni postavki 4. ponudbenega predračuna. Ta postavka ne črpa ur iz postavke »Podpora in dodatne storitve«.

Postavka »Osnovno vzdrževanje in odzivnost« zajema:

- zagotavljanje odzivnosti po principu 8x5 v obdobju 36 mesecev,
- redno spremljanje stanja rešitve in izvedba pregleda stanja najmanj enkrat na četrtoletje,
- nameščanje varnostnih popravkov, popravkov napak in stabilnih nadgradenj PAM rešitve,
- nameščanje popravkov oziroma nadgradenj operacijskega sistema in sistemskih komponent, kadar so te komponente del standardne postavitve ponujene rešitve,
- odprava napak v programski opremi in odprava znanih napak proizvajalca,
- obveščanje naročnika o varnostnih ranljivostih, priporočljivih posodobitvah in spremembah, ki vplivajo na delovanje rešitve.

6.2 Podpora in dodatne storitve

Podpora in dodatne storitve so namenjene aktivnostim, ki jih naročnik naroči zaradi operativnih potreb pri uporabi, spremembah ali širitvi rešitve. V ponudbenem predračunu je za te storitve predviden fond 504 ur za obdobje 36 mesecev.

Postavka »Podpora in dodatne storitve« zajema:

- pomoč pri uporabi in administraciji rešitve,
- spremembe nastavitvev, politik dostopa, skupin, vlog,odobritev in poročil,
- vključevanje dodatnih ciljnih sistemov, računov, skupin in scenarijev dostopa,
- pomoč pri odpravi težav, ki nastanejo zaradi sprememb konfiguracije, uporabniških nastavitvev ali sprememb v povezanih sistemih, ki jih izvede naročnik sam,
- svetovanje glede uporabe obstoječih funkcionalnosti ponujene rešitve,
- dopolnjevanje tehnične dokumentacije zaradi izvedenih sprememb.

Izvajalec mora mesečno pripraviti pregled porabljenih ur in izvedenih aktivnosti.

6.3 Odzivni časi

Osnovni zahtevani režim podpore je režim 8x5, med delovniki od 8. do 16. ure, z odzivnim časom za kritične napake največ 4 ure.

Prioriteta	Opis	Odzivni čas	Rok za vzpostavitev obvoda / odpravo napake
P1 - kritična	Nedelovanje produkcijskega sistema PAM ali kritična varnostna pomanjkljivost, zaradi katere ni mogoče varno izvajati privilegiranih dostopov.	4 ure	Obvod najkasneje naslednji delovni dan; trajna odprava po dogovoru z naročnikom in glede na kritičnost.
P2 - visoka	Moteno delovanje ključne funkcionalnosti brez primerne obkrožila ali večja degradacija delovanja.	8 delovnih ur	2 delovna dneva.
P3 - srednja	Motnja pri posamezni funkcionalnosti z obkrožila ali omejenim vplivom na delovanje.	2 delovna dneva	4 delovnih dni.

P4 - nizka	Manjša napaka, vprašanje, konfiguracijska sprememba, zahteva za svetovanje ali druga manj zahtevna storitev podpore.	3 delovne dni	6 delovnih dni.
------------	--	---------------	-----------------

7. ZAHTEVE GLEDE ZVOP-2, GDPR IN ZINPV-1

- Rešitev mora omogočati omejevanje dostopa do osebnih podatkov, revizijskih zapisov in posnetkov sej na pooblaščen osebe.
- Izvajalec mora pri izvedbi naročila ravnati skladno z GDPR, ZVOP-2, ZINPV-1 in internimi pravili naročnika s področja varstva osebnih podatkov in informacijske varnosti.
- Če izvajalec pri izvajanju pogodbe nastopa kot obdelovalec osebnih podatkov, mora biti obdelava urejena v skladu z 28. členom GDPR.
- Dostop do osebnih podatkov izven EU/EGP ni dopusten brez predhodnega pisnega soglasja naročnika in izpolnjenih pravnih pogojev.
- Izvajalec mora naročnika brez nepotrebne odlašanja in najkasneje v roku 4 ur obvestiti o zaznanih varnostnih ranljivostih, varnostnih napakah, incidentih ali drugih okoliščinah, ki bi lahko vplivale na varnost, zaupnost, celovitost ali razpoložljivost PAM rešitve.
- Izvajalec mora pri izvajanju naročila sodelovati z naročnikom pri izvedbi ukrepov, ki so potrebni za varno delovanje rešitve, odpravo ranljivosti, obvladovanje incidentov in zagotavljanje revizijske sledljivosti.

8. FAZE PROJEKTA IN PREVZEM

Implementacija projekta se izvede fazno. Spodnji terminski plan se po sklenitvi pogodbe uskladi s ponudnikom, pri čemer celotna implementacija ne sme presegati 6 mesecev od uvedbe v delo (T0).

Faza	Vsebina	Rok dokončanja	Zaključek faze
Faza 1 - Analiza in načrt	Pregled in popis obstoječega stanja, arhitektura, načrt implementacije, matrika odgovornosti.	T0+1 mesec	Potrjen dokument analize in načrt
Faza 2 - Testno okolje	Namestitev, osnovna konfiguracija, integracije, vključitev začetnega nabora ciljnih sistemov, testiranje v testnem okolju.	T0+3 meseci	Prevzem testnega okolja
Faza 3 - Produkcija	Priprava produkcijskega okolja, prenos konfiguracije, vključitev dogovorjenih sistemov, izobraževanja, prehod v produkcijo.	T0+5 mesecev	Produkcijski prehod
Faza 4 - Poskusno obratovanje	Stabilizacija, odprava napak, spremljanje delovanja, končna dokumentacija.	T0+6 mesecev	Končni prevzem