

Naša št.: 285-59/4-2026
Datum: 19. 8. 2026

TEHNIČNE SPECIFIKACIJE IN ZAHTEVE NAROČNIKA

Varnostna programska oprema, št. 285-59

SKLOP 1: UPRAVLJANJE DIGITALNIH POTRDIL

SKLOP 2: MODELIRANJE OMREŽJA, ANALIZA OMREŽNE IZPOSTAVLJENOSTI IN PREVERJANJE SEGMENTACIJE

SKLOP 3: SISTEM OBVEŠČANJA PREKO SMS SPOROČIL

SKLOP 4: ZAZNAVA IN OBVEŠČEVALNA PODPORA O KIBERNETSKIH GROŽNJAH (Kela CTI)

KAZALO

1	PREDMET IN TEHNIČNE ZAHTEVE JAVNEGA NAROČILA.....	3
2	TEHNIČNE SPECIFIKACIJE IN ZAHTEVE	4
2.1	SKLOP 1: UPRAVLJANJE DIGITALNIH POTRDIL – SWIM PKI	4
2.1.1	<i>Zahteve za sklop 1.....</i>	<i>4</i>
2.1.2	<i>Usposabljanje.....</i>	<i>8</i>
2.1.3	<i>Dokumentacija in testiranje.....</i>	<i>8</i>
2.1.4	<i>Garancija.....</i>	<i>8</i>
2.1.5	<i>Podpora.....</i>	<i>9</i>
2.1.6	<i>Reference ponudnika</i>	<i>9</i>
2.1.7	<i>Usposobljenost ponudnika</i>	<i>9</i>
2.1.8	<i>Rok dobave.....</i>	<i>9</i>
2.1.9	<i>Ostale zahteve za sklop 1</i>	<i>9</i>
2.2	SKLOP 2: CELOVITA REŠITEV ZA MODELIRANJE OMREŽJA, ANALIZO OMREŽNE IZPOSTAVLJENOSTI IN PREVERJANJE SEGMENTACIJE	10
2.2.1	<i>Zahteve za sklop 2.....</i>	<i>10</i>
2.2.2	<i>Dokumentacija in testiranje.....</i>	<i>14</i>
2.2.3	<i>Podpora.....</i>	<i>14</i>
2.2.4	<i>Rok dobave.....</i>	<i>14</i>
2.3	SKLOP 3: SISTEM OBVEŠČANJA PREKO SMS SPOROČIL	14
2.3.1	<i>Zahteve za sklop 3.....</i>	<i>15</i>
2.3.2	<i>Podpora.....</i>	<i>17</i>
2.3.3	<i>Rok dobave.....</i>	<i>18</i>
2.4	SKLOP 4: KELA CTI (PODALIŠANJE LICENCE)	19
2.4.1	<i>Zahteve za sklop 4.....</i>	<i>19</i>
2.4.2	<i>Dodatne zahteve za sklop 4</i>	<i>19</i>
2.4.3	<i>Rok in kraj dobave za sklop 4</i>	<i>19</i>
2.4.4	<i>Tehnična podpora proizvajalca in odzivni čas za sklop 4</i>	<i>19</i>

1 PREDMET IN TEHNIČNE ZAHTEVE JAVNEGA NAROČILA

Naročnik v okviru zagotavljanja visoke ravni kibernetske varnosti, neprekinjenega delovanja kritičnih informacijskih in operativnih sistemov, ter skladnosti z veljavnimi regulativnimi zahtevami (zlasti PART-IS, NIS2 in ISO/IEC 27001) izvaja predmetno javno naročilo za nakup, nadgradnjo in vzdrževanje obstoječih varnostnih rešitev.

Predmet javnega naročila tako zajema več sklopov, ki celovito naslavlajo ključna področja kibernetske varnosti:

- upravljanje digitalnih potrdil in zaupanja vredne infrastrukture,
- zagotavljanje skladnosti in revizijskih sledi z analizo mrežne izpostavljenosti,
- zanesljivo obveščanje ob varnostnih dogodkih in incidentih,
- zaznavo in obveščevalno podporo o kibernetskih grožnjah.

Naročilo vključuje nakup programske opreme za zgoraj naštetá področja.

Z izvedbo predmetnega naročila naročnik zasleduje naslednje ključne cilje:

- zgodnje zaznavanje in preprečevanje kibernetskih napadov,
- zmanjšanje tveganj, povezanih z dobavno verigo,
- povečanje odpornosti operativnih sistemov,
- zagotavljanje skladnosti z regulativnimi zahtevami,
- izboljšanje odzivnosti na incidente,
- zagotavljanje neprekinjenega in varnega delovanja ključnih storitev.

Posamezni sklopi javnega naročila so medsebojno povezani in tvorijo celovit varnostni ekosistem, ki naročniku omogoča proaktiven, centraliziran in dokazljiv pristop k upravljanju kibernetskih tveganj.

Natančne tehnične specifikacije in zahteve so opisane v nadaljevanju tega dokumenta.

2 TEHNIČNE SPECIFIKACIJE IN ZAHTEVE

2.1 Sklop 1: Upravljanje digitalnih potrdil – SWIM PKI

Predmet naročila sklopa 1 opredeljuje minimalne funkcionalne in tehnične zahteve za rešitev upravljanja digitalnih potrdil (angl. Certificate Lifecycle Management - CLM).

Rešitev mora podpirati celoten življenjski cikel digitalnih potrdil, vključno z izdajo, obnovo, preklicem in spremljanjem veljavnosti, ter omogočati varno upravljanje kriptografskih ključev. Poseben poudarek je na delovanju v segmentiranih in varnostno omejenih okoljih (IT, DMZ, OT), kjer neposreden dostop do interneta ni vedno zagotovljen.

Sistem mora omogočati integracijo z zunanjimi in notranjimi certifikacijskimi avtoritetami (Harica), podpirati standardne protokole za zaščito komunikacije (npr. TLS/mTLS) ter zagotavljati ustrezne mehanizme za beleženje, nadzor in revizijo vseh aktivnosti. Rešitev mora biti skladna z relevantnimi standardi in priporočili na področju SWIM PKI (European Aviation Common PKI) ter omogočati visoko razpoložljivost in varno delovanje v kritičnih okoljih zračnega prometa.

2.1.1 Zahteve za sklop 1

Postavka	Predmet	Zahteva
1	Nakup rešitve - Upravljanje digitalnih potrdil – SWIM PKI	Licenca, ki omogoča upravljanje vsaj 300 certifikatov za obdobje 36 mesecev
2	Podpora proizvajalca	Podpora proizvajalca za celoten sistem (vključno s posodobitvami in nadgradnjami) za obdobje najmanj 36 mesecev
3	Usposabljanje	Usposabljanje naročnikovega osebja za samostojno delo s ponujeno rešitvijo

Vse programske licence in podpora proizvajalca morajo biti veljavne za obdobje najmanj 36 mesecev.

2.1.1.1 Odkrivanje digitalnih potrdil

Rešitev mora podpirati odkrivanje in uvoz digitalnih potrdil prek naslednjih mehanizmov:

- Uvoz digitalnih potrdil iz imenika izdajatelja oziroma certifikacijske avtoritete (CA).
- Ročni uvoz digitalnih potrdil v obliki datoteke (npr. PEM, PFX, CER, CRT) prek uporabniškega vmesnika.
- Uvoz digitalnih potrdil prek programskega vmesnika (API)
- Pasivno odkrivanje digitalnih potrdil z neinvazivnim skeniranjem omrežnih naprav na določenih TCP/UDP vratih (angl. port scanning), brez vpliva na delovanje omrežja.
- Odkrivanje digitalnih potrdil na napravah z namestitvijo agenta (Windows in Linux).
- Odkrivanje potrdil v oblaknih okoljih (AWS, Azure, GCP) prek ustreznih API-jev.
- Odkrivanje potrdil v vsebnških okoljih (Kubernetes, Docker) in DevOps cevovodih (CI/CD).

2.1.1.2 Centralna evidenca digitalnih potrdil

Rešitev mora zagotavljati celovit in centraliziran pregled nad vsemi upravljanimi digitalnimi potrdili. Evidenca mora vsebovati vsaj naslednje podatke:

a. Atributi potrdila

- Skupno število upravljanih potrdil.

- Podpisni algoritmi, uporabljeni ob izdaji digitalnega potrdila (npr. RSA, ECDSA, SHA-256).
- Tip in dolžina kriptografskih ključev.
- Datum začetka veljavnosti, datum poteka in preostali čas veljavnosti potrdila.
- Izdajatelj digitalnega potrdila (CA in vmesni CA – chain of trust).
- Status potrdila (veljavno, poteklo, preklicano, nezaupano).
- Serijska številka potrdila in prstni odtis (fingerprint – SHA-1, SHA-256).
- Subject Alternative Names (SAN) in Common Name (CN).

b. Operativni podatki

- Lokacija namestitve digitalnega potrdila (strežnik, storitev, aplikacija, IP, FQDN).
- Skrbnik oziroma lastnik potrdila (posameznik ali skupina).
- Oznake (tags) in kategorije za grupiranje in iskanje potrdil.
- Revizijska sled sprememb na posameznem potrdilu.

c. Poročanje in skladnost

- Ustvarjanje poročil o skladnosti digitalnih potrdil z internimi varnostnimi politikami.
- Pregled potrdil, ki ne ustrezajo trenutnim standardom (zastareli algoritmi, prekratki ključi, iztekla veljavnost, samo-podpisana potrdila ipd.).
- Izvoz podatkov o potrdilih v standardnih formatih (CSV, JSON, PDF).
- Možnost načrtovanja in avtomatskega pošiljanja periodičnih poročil.

2.1.1.3 Upravljanje dostopov

Rešitev mora omogočati granularno upravljanje dostopov z upoštevanjem načela najmanjših pravic (Principle of Least Privilege):

a. Vloge in pravice

- Vzpostavitev ločenih vlog: administrator rešitve, skrbnik potrdil, pregledovalec (read-only) in vlagatelj zahtev.
- Ustvarjanje skupin/ekip skrbnikov digitalnih potrdil z dodeljevanjem potrdil posameznim skupinam.
- Ločevanje administrativnih in operativnih vlog – skrbnik potrdil ne sme imeti dostopa do sistemske administracije.
- Podpora za večstopenjsko odobravanje zahtev (angl. approval workflow).

b. Integracija z imeniki

- Integracija z Microsoft Active Directory prek protokola LDAP/LDAPS.
- Uvoz obstoječih uporabnikov in uporabniških skupin iz AD.

2.1.1.4 Visoka razpoložljivost in odpornost na napake

- Rešitev mora podpirati delovanje v visoko razpoložljivem grozdu (HA Cluster) brez izpada storitve ob odpovedi posameznega vozlišča.
- Podpora za aktivno-aktivno (Active-Active) ali aktivno-pasivno (Active-Passive) konfiguracijo.
- Podpora za geografsko ločeni lokaciji (disaster recovery).
- Rešitev mora podpirati redno varnostno kopiranje konfiguracije in podatkov (backup) ter obnovitev iz varnostne kopije (restore).

2.1.1.5 Upravljanje življenjskega cikla digitalnih potrdil

Rešitev mora podpirati upravljanje celotnega življenjskega cikla digitalnih potrdil – od zahteve za izdajo, prek obnove, do upokojitve in preklica.

a. Splošne zahteve

- Avtomatizirano obnavljanje potrdil pred njihovim potekom (brez ročnega posredovanja).
- Upravljanje ključev: generiranje, shranjevanje in zaščita zasebnih ključev.
- Podpora za upravljanje CSR (Certificate Signing Request).
- Podpora za preklicanje (revokacijo) potrdil.
- Podpora za validacijo potrdil prek CRL in OCSP.

b. Javni izdajatelji (Public CA)

Rešitev mora podpirati integracijo z vsaj naslednjimi javnimi certifikacijskimi avtoritetami:

- Amazon Certificate Manager (ACM)
- Sectigo Certificate Manager (SCM)
- DigiCert CertCentral
- Entrust Certificate Services
- GlobalSign MSSL
- HID PKIaaS
- QuoVadis
- VikingCloud
- ACMEv2 (RFC 8555) – podpora za avtomatizirano izdajo in obnovo potrdil

c. Zasebni izdajatelji (Private / Internal CA)

Rešitev mora podpirati integracijo z vsaj naslednjimi zasebnimi certifikacijskimi avtoritetami:

- Prilagodljiva CA po meri (Adaptable CA) – možnost integracije z nestandardnimi CA prek skriptnega vmesnika
- Microsoft Standalone CA
- Microsoft Enterprise CA (Active Directory Certificate Services – ADCS)
- OpenSSL
- OpenTrust Enterprise PKI
- RedHat Certificate System
- RSA Certificate Manager
- DigiCert PKI Platform
- HashiCorp Vault PKI (zaželeno)
- EJBCA (zaželeno)

2.1.1.6 Nameščanje digitalnih potrdil

Rešitev mora podpirati avtomatizirano nameščanje digitalnih potrdil v ciljne storitve in aplikacije.

a. Generične namestitve brez agenta

- Nameščanje prek protokola SSH na Linux/Unix naprave.
- Nameščanje prek protokola WinRM na Windows naprave.
- Nameščanje v Windows Certificate Store.
- Podprti formati: PKCS#8, PKCS#12 (PFX), PEM, DER, JKS.
- Možnost nastavitve poti (path) in dovoljenj datoteke na ciljnim sistemu.

b. Nameščanje z agentom

- Nameščanje z lahkotnim agentom na naprave Windows in Linux.
- Nameščanje v Windows Certificate Store.
- Podprti formati: PKCS#8, PKCS#12 (PFX), PEM, DER, JKS.
- Možnost nastavitve poti (path) in dovoljenj datoteke na ciljnem sistemu.

c. Integrirano nameščanje v aplikacije in infrastrukturo

Rešitev mora podpirati direktno nameščanje v vsaj naslednje rešitve:

- Microsoft IIS (Internet Information Services)
- Apache HTTP Server
- NGINX
- F5 BIG-IP (LTM/GTM)
- Citrix NetScaler / ADC
- VMware NSX / vSphere
- AWS (ACM, IAM, ALB/ELB)
- Azure Key Vault
- Kubernetes (cert-manager, Secrets)
- HashiCorp Vault
- Palo Alto Networks
- Imperva

2.1.1.7 Obveščanje in alarmiranje

Rešitev mora omogočati proaktivno obveščanje skrbniških skupin in posameznih skrbnikov o vsaj naslednjih dogodkih:

a. Dogodki, ki sprožijo obvestila

- Bližajoči se potek veljavnosti potrdila (nastavljivi pragovi, npr. 90, 60, 30, 14, 7 dni).
- Pretečena veljavnost potrdila.
- Neuspešna validacija potrdila (npr. potrdilo ni zaupano, napaka v verigi, preklic).
- Uspešna ali neuspešna namestitev potrdila.
- Neuspešna obnova potrdila.
- Zahteva po avtorizaciji akcije (odobritev zahteve za izdajo ali obnovo).
- Odkritje novega potrdila pri skeniranju.
- Sprememba konfiguracije ali politike.
- Varnostna opozorila (npr. zaznan šibek ključ, zastareli algoritem).

b. Kanali dostave obvestil

- E-pošta (SMTP).
- Syslog (UDP/TCP).
- Integracija s sistemi za upravljanje opravil ali incidentov.
- Zapis obvestil v podatkovno bazo.

2.1.1.8 Varnostne zahteve

- Vsa komunikacija med komponentami rešitve mora biti šifrirana (TLS 1.2 ali višje).
- Zasebni ključi morajo biti zaščiteni v šifrirani obliki; podpora/integracija za HSM (Hardware Security Module) proizvajalca Utimaco.
- Revizijska sled (audit log) vseh akcij v sistemu z možnostjo izvoza.
- Podpora za varne seje (timeout neaktivnih sej, obveščanje o napačnih prijavah).

- Skladnost z zahtevami standardov ISO 27001 in eIDAS (kjer relevantno).

2.1.1.9 Integracije in interoperabilnost

- API za vse ključne operacije (izdaja, obnova, preklic, pregled potrdil).
- Podpora za protokol ACME (RFC 8555) za avtomatizirano upravljanje potrdil.
- Podpora za protokol SCEP (Simple Certificate Enrollment Protocol).
- Podpora za protokol EST (Enrollment over Secure Transport, RFC 7030) .
- Integracija z SIEM sistemi prek Syslog.
- Podpora za Kubernetes cert-manager.

2.1.1.10 Zahteve glede infrastrukture za namestitev

- Namestitev na lokalni infrastrukturi (on premises) na operacijskem sistemu Windows Server.
- Jasno dokumentirani sistemski predpogoji (CPU, RAM, disk, omrežje).
- Podpora za podatkovne baze Microsoft SQL Server.

2.1.2 Usposabljanje

Zahteva se izvedba osnovnega tehničnega, ti. »hands on« usposabljanja na lokaciji naročnik (Zg. Brnik 130n, 4210 Brnik – aerodrom) za osebje naročnika. Usposabljanja se bo udeležilo 4 do največ 6 udeležencev – osebje naročnika.

Usposabljanje mora trajati 2 delovna dneva po 6 ur (1 ura je 60 minut).

Usposabljanje mora vključevati naslednje teme:

- osnovni koncepti PKI in CLM (CA, certifikati, CRL, OCSP, TLS/mTLS),
- upravljanje življenjskega cikla potrdil (izdaja, obnova, preklic),
- konfiguracijo in upravljanje CLM sistema,
- integracija z drugimi sistemi (npr. aplikacije, strežniki, HSM, SIEM),
- upravljanje dostopa in vlog (RBAC),
- pregled logov, nadzor in osnovno odpravljanje napak.

Usposabljanje mora vključevati tudi simulacijo realnih operativnih scenarijev (npr. potek potrdila, preklic kompromitiranega certifikata, izpad povezave do validacijskih storitev) ter odziv naročnikove ekipe na takšne dogodke. Usposabljanje mora vključevati teoretični in praktični (hands-on) del. Usposabljanje mora biti izvedeno na dejanski implementirani rešitvi ali v enakovrednem testnem okolju.

2.1.3 Dokumentacija in testiranje

Najpozneje ob primopredaji opreme, t.j. po uspešnem testiranju, je izvajalec dolžan naročniku izročiti ustrezno tehnično dokumentacijo, ki mora obsegati najmanj:

- opis dobavljene opreme

2.1.4 Garancija

Zahtevana garancijska doba je 36 mesecev od uspešne primopredaje, t.j. ko naročnik podpiše zapisnik o uspešni primopredaji.

2.1.5 Podpora

Podpora proizvajalca, ki je zahtevana v razpisu, mora biti na voljo na lokaciji naročnika ter za celotno obdobje trajanja pogodbe.

Podpora proizvajalca mora vključevati:

- Odzivni čas v režimu 8×5 NBD (Next Business Day)

2.1.6 Reference ponudnika

Ponudnik mora izkazati, da je v zadnjih treh (3) letih implementiral vsaj 1 referenčno postavitven sistem, ki ga ponuja, v produkcijskem okolju z vsaj 300 certifikatov) na območju Republike Slovenije.

Upošteevane bodo le tiste reference, za katere bo priložena izjava končnega naročnika, potrjena na obrazcu naročnika. Naročnik si pridrukuje pravico, da preveri resničnost navedenih referenc pri navedenih naročnikih. V primeru neresničnih ali zavajajočih navedb bo naročnik ponudbo izločil iz nadaljnje obravnave.

2.1.7 Usposobljenost ponudnika

Usposobljenost ponudnikovega kadra za instalacijo, konfiguriranje, vzdrževanje, tehnično podporo opreme ponujenega proizvajalca:

- Ponudnik mora za najmanj eno (1) tehnično strokovno osebo (strokovnjak) izkazati, da ima veljavno potrdilo/certifikat proizvajalca ponujene opreme, da je opravil usposabljanje oz. je usposobljen za upravljanje in konfiguracijo ponujene rešitve.

Vsi strokovnjaki, ki bodo sodelovali na projektu morajo aktivno govoriti slovenski jezik (nivo B2 v skladu s CEFR), naročnik pa si pridrukuje pravico, da od ponudnika glede tega zahteva ustrezna dokazila.

2.1.8 Rok dobave

Rok dobave za ponujeno programsko opremo znaša 30 koledarskih dni po sklenitvi pogodbe.

2.1.9 Ostale zahteve za sklop 1

Ponudnik mora predložiti izjavo (angl. MAF) odgovorne osebe/proizvajalca ali uradnega zastopnika za območje Slovenije, da ima ponudnik s proizvajalcem ponujene opreme sklenjeno veljavno pogodbo, ki zajema tako dobavo opreme/licenc, kot tudi celotno podporo (dostop) do tehnične pomoči, dostop do baze znanj, za blagovno znamko, ki jo ponuja.

2.2 Sklop 2: Celovita rešitev za modeliranje omrežja, analizo omrežne izpostavljenosti in preverjanje segmentacije

Sklop 2 se nanaša na uvedbo sistema za celovito analizo omrežne topologije, preverjanje dostopnosti med sistemi ter identifikacijo varnostnih tveganj, ki izhajajo iz konfiguracij omrežne infrastrukture (enakovredno kot je npr. ReadSeal).

Namen naročnika je vzpostaviti centralni sistem, ki omogoča celovit in zanesljiv vpogled v dejansko omrežno izpostavljenost informacijskega okolja ter preverjanje pravilnosti implementirane segmentacije med posameznimi omrežnimi območji.

Naročnik želi z uvedbo rešitve doseči:

- jasno razumevanje dejanskih komunikacijskih poti med sistemi, ne glede na kompleksnost omrežne infrastrukture,
- identifikacijo vseh možnih dostopnih poti med omrežnimi segmenti (tudi nenamernih ali napačno konfiguriranih),
- preverjanje učinkovite ločitve med različnimi varnostnimi conami (npr. IT, DMZ, OT, IoT),
- pravočasno odkrivanje nepravilnosti v konfiguracijah omrežnih naprav, ki lahko vodijo do varnostnih tveganj,
- podporo pri analizi vpliva sprememb v omrežju pred njihovo implementacijo,
- izboljšanje nadzora nad skladnostjo z internimi varnostnimi politikami ter regulatornimi zahtevami.

Rešitev mora omogočati analizo omrežja na podlagi konfiguracij omrežnih naprav ter zagotavljati natančen model omrežja, ki omogoča simulacijo dostopnosti med sistemi in identifikacijo potencialnih napadalnih poti.

Poseben poudarek je na okoljih z visoko stopnjo segmentacije in heterogeno infrastrukturo, kjer naročnik potrebuje zanesljivo orodje za preverjanje dejanskega stanja, neodvisno od posameznih proizvajalcev omrežne opreme.

2.2.1 Zahteve za sklop 2

Postavka	Predmet	Zahteva	Količina
1	Nakup licence za 1 leto – letna naročnina	Letna naročnina za eno napravo na nivoju L3 (Layer 3) za obdelavo paketov	25
2	Nakup licence za 1 leto – letna naročnina	Letna naročnina za eno napravo na nivoju L2 (Layer 2), ki vključuje tudi funkcionalnost Incident Response	150
3	Nakup licence za 1 leto – letna naročnina	Letna naročnina za dostop do vseh razpoložljivih CIS vsebin za nivoja L3 in L2	25
4	Nakup licence za 1 leto – letna naročnina	Letna naročnina za modul za upravljanje delovnih tokov (workflow), ki omogoča avtomatizacijo ročnih postopkov ter integracijo z drugimi sistemi	1

Izbrani ponudnik bo za obdobje 12 mesecev zagotovil veljavne licence za uporabo ponujene programske rešitve ter pripadajoče dostope do vseh funkcionalnosti in vsebin, ki jih rešitev nudi v okviru naročene licence.

Ponudnik bo zagotavljal tudi, da ima naročnik v času trajanja pogodbe neprekinjen dostop do posodobitev in nadgrajenij platforme, ki jih v okviru storitve zagotavlja proizvajalec, brez dodatnih vplivov na obstoječe podatke in delovanje sistema.

Ponudnik mora za vsako zahtevo v tehnični specifikaciji navesti izpolnjevanje zahteve in predložiti dokazilo oziroma sklic na uradno proizvajalčevo dokumentacijo, tehnični opis, zaslonski prikaz, izjavo proizvajalca ali drugo ustrezno dokazilo.

2.2.1.1 Splošne zahteve

- Rešitev mora delovati kot programska oprema, ki se namesti v virtualnem okolju naročnika.
- Rešitev mora omogočati centralizirano analizo omrežne infrastrukture.
- Rešitev mora biti neodvisna od proizvajalca omrežne opreme (multi-vendor).
- Rešitev mora omogočati delovanje brez potrebe po aktivnem poseganju v produkcijsko omrežje (brez inline namestitve oziroma pomožnih agentov).
- Rešitev mora temeljiti na analizi konfiguracijskih podatkov omrežnih naprav.
- Rešitev mora podpirati federirano arhitekturo namestitve, ki omogoča, da več ločenih (izoliranih) instanc platforme (npr. po posameznih omrežnih varnostnih conah) deli modelirane podatke s centralno upravljavsko instanco, ne da bi bila med conami potrebna neposredna omrežna povezljivost.
- Rešitev mora omogočati popolno namestitev v lokalnem okolju (on-premises), brez potrebe po povezljivosti v oblak, uporabi oblačnih komponent ali prenosu podatkov izven omrežnega perimetra organizacije. Vsi podatki — vključno z omrežno topologijo, podatki o ranljivostih in konfiguracijskimi datotekami — morajo ves čas ostati znotraj infrastrukture organizacije.
- Rešitev mora podpirati nadzor dostopa na podlagi vlog (RBAC) z najmanj naslednjimi vlogami: sistemski administrator, administrator modela, varnostni analitik in uporabnik z vpogledom (read-only). Vsi dostopi morajo biti beleženi.
- Rešitev mora omogočati integracijo z imeniki podjetja (Active Directory/LDAP) za avtentikacijo uporabnikov ter podpirati SAML 2.0 ali OpenID Connect (OIDC) za enotno prijavo (SSO).
- Vsi podatki v prenosu med komponentami rešitve ter med rešitvijo in nadzorovanimi napravami morajo biti šifrirani z uporabo TLS 1.2 ali novejšega. Vsi podatki v mirovanju morajo biti šifrirani z uporabo AES-256 ali enakovrednega algoritma.

2.2.1.2 Zbiranje podatkov

- Rešitev mora omogočati uvoz konfiguracij iz:
 - požarnih zidov (firewall), load balancerjev, WAF, ...
 - usmerjevalnikov prometa,
 - stikal,
 - virtualnih omrežnih komponent.
- Rešitev mora podpirati več proizvajalcev omrežne opreme (standardne proizvajalce).
- Rešitev mora omogočati avtomatiziran (SSH, SFTP, SCP, SMB) in ročni uvoz konfiguracij.
- Rešitev mora omogočati načrtovano in samodejno zbiranje podatkov ob poljubno določenem času ter tudi ročno sprožitev zbiranja po potrebi.
- Rešitev mora omogočati periodično osveževanje podatkov.
- Rešitev mora omogočati delovanje na osnovi offline konfiguracij (brez potrebe po real-time prometu).
- Rešitev mora omogočati zajem podatkov o ranljivostih iz orodij tretjih ponudnikov in agentskih rešitev na končnih točkah, vključno z Tenable (Nessus / Tenable.sc / Tenable.io), Qualys, Rapid7 InsightVM, CrowdStrike Falcon, Microsoft Defender ter Dragos (za podatke o ranljivostih OT sredstev).
- Za odkrivanje sredstev v OT okoljih mora rešitev omogočati zajem podatkov o sredstvih in ranljivostih iz namenskih OT/ICS varnostnih platform, kot so Dragos, Nozomi Networks in Claroty, z namenom obogatitve omrežnega modela s podatki o napravah PLC, RTU in IED.

2.2.1.3 Modeliranje omrežja

- Rešitev mora omogočati izgradnjo natančnega modela omrežja. Omogočati mora vpogled na nivoju posamezne naprave, vključno z: konfiguracijami vmesnikov, IP-naslabljanjem, usmerjevalnimi tabelami, pravili ACL/požarnega zidu, dodelitvami VLAN, MAC tabelami ter ARP tabelami — vse v poenoteni, proizvajalčno neodvisni obliki, ki ne zahteva poznavanja specifične CLI sintakse posameznega proizvajalca.
- Model mora vključevati:
 - L2 segmente,
 - L3 povezave,
 - routing logiko,
 - firewall pravila.
- Rešitev mora vzpostaviti in vzdrževati stalno posodobljen digitalni dvojček (digital twin) hibridnega omrežnega okolja organizacije, ki natančno odraža vse naprave na nivoju plasti 2 in 3, njihove medsebojne povezave, usmerjevalne poti, sezname za nadzor dostopa (ACL), požarne politike, NAT pravila ter cone omrežne segmentacije.
- Digitalni dvojček mora omogočati vizualni prikaz omrežne topologije v obliki interaktivnega zemljevida, ki podpira hierarhično razvrščanje naprav po conah, segmentih ali funkcijah (npr. OT cona 1, OT cona 2, IT DMZ, korporativni LAN, IoT), pri čemer mora biti struktura prilagodljiva s strani administratorjev.
- Rešitev mora omogočati modeliranje kompleksnih topologij (multi-hop).
- Rešitev mora omogočati prikaz poti skozi več zaporednih omrežnih naprav.
- Rešitev mora omogočati modeliranje hibridnih okolij (fizično + virtualno).
- Rešitev mora prepoznati in jasno označiti omrežne segmente, podomrežja ali gostitelje, za katere ne obstajajo podatki o skeniranju ranljivosti (t. i. »temni prostor«), ter s tem izpostaviti morebitne vrzeli v programu upravljanja ranljivosti organizacije.
- Rešitev mora pravilno modelirati in obravnavati več nivojski omrežni prevod naslovov (NAT), pri čemer mora natančno prikazovati tako izvirne (pre-NAT) kot prevedene (post-NAT) IP naslove v celotnem omrežnem modelu in vseh poizvedbah.

2.2.1.4 Analiza dostopnosti (path analysis)

- Rešitev mora omogočati deterministično analizo dejanske omrežne dostopnosti med sistemi na podlagi konfiguracijskih podatkov.
- Rešitev mora omogočati:
 - identifikacijo vseh možnih komunikacijskih poti,
 - analizo poti skozi več naprav,
 - identifikacijo nenamernih povezav.
- Rešitev mora omogočati preverjanje dostopnosti med:
 - posameznimi IP naslovi,
 - omrežnimi segmenti,
 - varnostnimi conami.
- Rešitev mora omogočati simulacijo dostopnosti brez generiranja prometa.
- Rešitev mora omogočati določitev vseh možnih dostopnih poti med poljubno izbranim izvorom in ciljem v omrežnem modelu, pri čemer mora upoštevati dejanske konfiguracije naprav, pravila ACL, politike požarnih zidov, usmerjevalne tabele in NAT — ne zgolj najkrajše ali primarne poti.

2.2.1.5 Preverjanje segmentacije

- Rešitev mora omogočati preverjanje ločitve med varnostnimi conami.
- Rešitev mora omogočati:
 - preverjanje IT–DMZ–OT–IoT segmentacije,
 - identifikacijo kršitev segmentacije,
 - preverjanje skladnosti z varnostnimi politikami.
- Rešitev mora omogočati definiranje pravil dovoljenih in nedovoljenih komunikacij.

- Rešitev mora podpirati zaznavanje asimetričnega usmerjanja, pri čemer identificira primere, ko se poti v smeri od izvora do cilja in nazaj razlikujejo.
- Rešitev mora modelirati tako enosmeren kot dvosmeren dostop med omrežnimi conami ter podpirati specifične arhitekture, kot se uporabljajo v ATC okoljih, vključno z enosmernimi podatkovnimi diodami, kjer je to relevantno.

2.2.1.6 Analiza tveganj

- Rešitev mora omogočati identifikacijo potencialnih napadalnih poti.
- Rešitev mora omogočati analizo dosega (t. i. »blast radius«), kjer na podlagi izbranega izvora ali kompromitiranega sistema identificira vse dosegljive cilje v omrežju ter rezultat prikaže tako v obliki seznama kot tudi na topološkem zemljevidu.
- Rešitev mora omogočati analizo varnostnega vpliva pred uvedbo sprememb (pre-deployment), kjer za predlagano pravilo požarnega zidu ali spremembo konfiguracije izračuna in prikaže:
 - število in naravo novih dostopnih poti,
 - število predhodno nedosegljivih ranljivosti, ki postanejo dosegljive,
 - število gostiteljev, ki so na novo izpostavljeni nezaupanja vrednim omrežjem,
 - morebitne kršitve pravil omrežne segmentacije.
- Rešitev mora omogočati prioriteto razvrščanje tveganj.
- Rešitev mora omogočati povezovanje omrežnih poti s kritičnostjo sistemov.
- Rešitev mora omogočati integracijo s katalogom CISA Known Exploited Vulnerabilities Catalog (KEV) — bodisi neposredno bodisi preko avtomatiziranih procesov — za prepoznavanje in prioriteto obravnavo ranljivosti z potrjeno aktivno zlorabo v praksi.
- Rešitev mora spremljati stanje tveganj skozi čas ter omogočati analizo trendov, ki prikazuje izboljšanje ali poslabšanje skupne ocene tveganja organizacije v izbranih časovnih obdobjih.

2.2.1.7 Analiza sprememb (change impact analysis)

- Rešitev mora omogočati simulacijo sprememb v omrežju.
- Rešitev mora omogočati:
 - analizo vpliva sprememb firewall pravil,
 - preverjanje vpliva sprememb routing konfiguracij,
 - oceno tveganja pred implementacijo spremembe.
- Rešitev mora omogočati spremljanje in poročanje o spremembah konfiguracij naprav med posameznimi cikli zbiranja podatkov ter zagotavljati jasen prikaz razlik (diff), ki vključuje dodane, spremenjene in odstranjene konfiguracijske vrstice.

2.2.1.8 Vizualizacija

- Rešitev mora omogočati grafični prikaz omrežne topologije.
- Rešitev mora omogočati:
 - vizualizacijo poti med sistemi,
 - prikaz varnostnih con,
 - pregled kompleksnih povezav.
- Rešitev mora omogočati interaktivno raziskovanje omrežja.
- Rešitev mora ob vsakem zaključenem ciklu zbiranja podatkov takoj zaznati in jasno označiti morebitne kršitve definiranih segmentacijskih politik — preko nadzorne plošče in nastavljenih obvestil.

2.2.1.9 Integracije

- Rešitev mora omogočati integracijo z:
 - SIEM sistemi,
 - sistemi za upravljanje ranljivosti,
 - sistemi za upravljanje konfiguracij.
- Rešitev mora omogočati izvoz podatkov preko API ali enakovrednih vmesnikov.

- Rešitev mora omogočati integracijo z drugimi varnostnimi orodji.
- Rešitev mora omogočati izvoz modela omrežne topologije v najmanj dveh formatih, primernih za dokumentiranje in revizijo (npr. Visio, PDF, SVG, CSV inventar).
- Rešitev mora omogočati generiranje poročil o skladnosti, ki jih je mogoče izvoziti najmanj v formatih PDF in CSV, primernih za interno revizijo, vodstvo, EUROCONTROL ter nacionalne nadzorne organe v okviru NIS2 Directive.
- Rešitev mora zagotavljati agregirano metriko varnostnega stanja (npr. »Digital Resilience Score«), ki se spremlja skozi čas in je primerna za poročanje vodstvu ter regulatornim organom.
- Rešitev mora podpirati avtomatizirano obogatitev incidentov — ob prejemu indikatorja kompromitacije (IoC) ali alarma iz zunanjega sistema (npr. SIEM, EDR) mora platforma samodejno poizvedeti po svojem modelu ter vrniti: lokacijo sredstva, trenutno cono, dosegljive cone, povezane ranljivosti in lastništvo sistema — vse kot prilogo izvirnega alarma ali zahtevka.

2.2.1.10 Razširljivost in zmogljivost

- Rešitev mora podpirati okolja z velikim številom naprav in segmentov.
- Rešitev mora omogočati analizo kompleksnih omrežij z več nivoji segmentacije.
- Rešitev mora omogočati razširitev na dodatne naprave brez degradacije delovanja.

2.2.1.11 Arhitekturna zahteva

- Rešitev mora temeljiti na modelu omrežja, ki se gradi na osnovi konfiguracijskih podatkov.
- Rešitev mora omogočati analizo omrežja brez potrebe po zajemu ali analizi dejanskega prometa.
- Rešitev mora omogočati natančno rekonstrukcijo komunikacijskih poti skozi omrežje.

2.2.2 Dokumentacija in testiranje

Najpozneje ob podpisu primopredajnega zapisnika za programsko opremo, je ponudnik dolžan naročniku izročiti ustrezno tehnično dokumentacijo, ki mora obsegati najmanj:

- opis dobavljene opreme
- dokumentiran REST API za integracijo s sistemi tretjih ponudnikov, z avtentikacijo preko API ključev, OAuth 2.0 ali enakovrednega mehanizma. API dokumentacija mora biti naročniku na voljo ob dobavi.

2.2.3 Podpora

Podpora proizvajalca, mora biti za celotno obdobje trajanja licence in mora vključevati:

- Odzivni čas v režimu 8×5 NBD (Next Business Day)

2.2.4 Rok dobave

Rok dobave za ponujeno programsko opremo znaša 30 koledarskih dni po sklenitvi pogodbe.

2.3 Sklop 3: Sistem obveščanja preko SMS sporočil

Sklop 3 se nanaša na implementacijo sistema za centralizirano sprejemanje, obdelavo in posredovanje sporočil preko SMS komunikacijskega kanala. Namen rešitve je zagotoviti zanesljivo dvosmerno komunikacijo, kjer sistem omogoča tako pošiljanje, kot tudi sprejemanje sporočil ter njihovo nadaljnjo obdelavo in distribucijo na podlagi vnaprej definiranih pravil.

Rešitev mora omogočati integracijo z obstoječimi informacijskimi sistemi in aplikacijami ter podpirati avtomatizirano obdelavo vhodnih sporočil (npr. parsiranje vsebine, proženje dogodkov, posredovanje drugim sistemom ali uporabnikom). Sistem mora zagotavljati sledljivost vseh prejetih in poslanih sporočil, upravljanje prejemnikov ter možnost definiranja komunikacijskih tokov.

Rešitev se mora integrirati z obstoječo SMS infrastrukturo naročnika, in sicer z napravo SMSEagle, ter podpirati njene standardne vmesnike za pošiljanje in sprejemanje sporočil.

Poseben poudarek je na zanesljivosti dostave, pravočasni obdelavi vhodnih sporočil ter uporabi v okoljih, kjer je SMS komunikacija ključni mehanizem za obveščanje, upravljanje ali interakcijo z uporabniki in sistemi.

2.3.1 Zahteve za sklop 3

Postavka	Predmet	Zahteva
1	Programska oprema	Celovita rešitev alarmiranja in obveščanja tako kot je navedeno v tehničnih specifikacijah
2	Storitve svetovanja v obsegu 30 ur	Pomoč pri integraciji in konfiguraciji sistema v okviru 30 ur

Naročnik kupuje programsko rešitev za sprejem, obdelavo in posredovanje SMS sporočil, ki bo delovala v virtualnem okolju na operacijskem sistemu Windows Server. Rešitev mora biti dobavljena kot programska oprema, ki se namesti na obstoječo strežniško infrastrukturo naročnika, brez potrebe po namenski ali specializirani strojni opremi.

2.3.1.1 Splošne zahteve

- Rešitev mora delovati kot centralni strežniški sistem za sprejemanje, obdelavo in pošiljanje SMS sporočil ter podpirati dvosmerno komunikacijo.
- Rešitev mora delovati kot storitev (service) brez potrebe po aktivni uporabniški seji ter omogočati sočasno obdelavo več komunikacijskih tokov.
- Rešitev mora delovati kot centralni sistem za obdelavo sporočil, kjer so sprejem, obdelava in posredovanje sporočil med seboj logično ločeni.
- Rešitev mora omogočati obdelavo sporočil kot samostojnih entitet, ki imajo definiran življenjski cikel od sprejema do končne dostave.
- Rešitev mora zagotavljati trajno shranjevanje sporočil skozi celoten življenjski cikel ter omogočati nadaljevanje obdelave po ponovnem zagonu sistema brez izgube podatkov.
- Rešitev mora vključevati lasten mehanizem za upravljanje čakalnih vrst (message queue), ki zagotavlja zanesljivo obdelavo sporočil.

2.3.1.2 Sprejem sporočil

- Rešitev mora omogočati hkraten sprejem sporočil iz več različnih vhodnih virov.
- Podprti morajo biti najmanj naslednji načini:
 - sprejem preko e-pošte (SMTP),
 - sprejem preko HTTP/HTTPS API,
 - sprejem preko datotečnega sistema (file drop/pickup mehanizem),
 - sprejem iz relacijskih baz podatkov ali preko standardnih podatkovnih vmesnikov,
 - sprejem preko spletne strani
 - sprejem preko ukazne vrstice (CLI) ali skript,
 - sprejem preko serijskih komunikacijskih vmesnikov,
 - sprejem preko SNMP trap sporočil.
- Rešitev mora omogočati sprejem SNMP trap sporočil ter njihovo pretvorbo v obdelovalna sporočila znotraj sistema.

- Rešitev mora omogočati sočasno aktivno uporabo vseh navedenih vhodnih mehanizmov, pri čemer mora biti vsak vhod obravnavan kot neodvisen vir dogodkov.

2.3.1.3 Obdelava in logika sporočil

- Rešitev mora vsebovati vgrajen sistem pravil (rule engine), ki omogoča napredno obdelavo sporočil.
- Rešitev mora omogočati večstopenjsko obdelavo sporočil, kjer se posamezno sporočilo obdeluje skozi zaporedje definiranih korakov.
- Rešitev mora omogočati:
 - definiranje pravil na podlagi več pogojev hkrati (npr. vsebina, pošiljatelj, vir, čas),
 - pogojno logiko (if/then/else),
 - transformacijo/prevod vsebine sporočil,
 - razdelitev enega vhodnega sporočila na več izhodnih sporočil,
 - razvejanje sporočil na več izhodnih poti ali prejemnikov,
 - sprožanje več neodvisnih akcij na podlagi enega vhodnega sporočila.
- Rešitev mora omogočati centralno upravljanje vseh pravil in komunikacijskih tokov.

2.3.1.4 Enoten obdelovalni mehanizem

- Rešitev mora zagotavljati, da se vsi vhodni viri (npr. IT sistemi, varnostni sistemi, sistemi fizične varnosti, SOC, energetski sistemi) obdelujejo preko enotnega mehanizma za obdelavo sporočil.
- Obdelava sporočil ne sme biti odvisna od tipa vhodnega sistema, temveč mora biti centralizirana in enotna.

2.3.1.5 Pošiljanje sporočil

- Rešitev mora omogočati pošiljanje SMS sporočil posameznikom in skupinam uporabnikov.
- Rešitev mora omogočati uporabo več izhodnih komunikacijskih kanalov hkrati.
- Rešitev mora omogočati:
 - pošiljanje istega sporočila na več različnih izhodnih poti,
 - samodejni preklon na alternativni komunikacijski kanal v primeru nedosegljivosti primarnega,
 - ponovno pošiljanje sporočil (retry mehanizem),
 - prioritizirano obdelavo sporočil,
 - časovno načrtovanje pošiljanja (scheduling).

2.3.1.6 Zanesljivost in nadzor nad sporočili

- Rešitev mora zagotavljati popoln nadzor nad stanjem posameznega sporočila (npr. sprejeto, v obdelavi, poslano, neuspešno).
- Rešitev mora omogočati:
 - upravljanje čakalnih vrst,
 - ponovno pošiljanje sporočil,
 - spremljanje statusa dostave,
 - prioritizacijo sporočil,
 - nadaljevanje obdelave po izpadu sistema brez izgube podatkov.

2.3.1.7 Integracija z varnostnimi in IT sistemi

- Rešitev mora omogočati integracijo z varnostnimi sistemi (npr. SOC, SIEM, sistemi fizične varnosti) ter podpirati obdelavo dogodkov iz teh sistemov v realnem času.
- Rešitev mora omogočati integracijo z OpenText Operations Agent oziroma enakovrednim sistemom za upravljanje dogodkov, pri čemer mora omogočati sprejem dogodkov (eventov) ter njihovo pretvorbo v obdelovalna sporočila in nadaljnje posredovanje v obliki SNMP trapa.
- Rešitev mora omogočati pretvorbo dogodkov iz različnih sistemov v strukturirana sporočila ter njihovo nadaljnjo obdelavo in distribucijo.

- Rešitev mora omogočati, da se dogodki iz različnih sistemov na podlagi definiranih pravil posredujejo različnim skupinam uporabnikov ali drugim sistemom.

2.3.1.8 Integracijski vmesniki

- Rešitev mora omogočati integracijo preko različnih standardnih vmesnikov, vključno z:
 - API (HTTP/HTTPS),
 - e-pošta,
 - datotečni sistem,
 - relacijske baze podatkov,
 - ukazna vrstica,
 - SNMP (sprejem trap sporočil),
 - serijski komunikacijski vmesniki (RS-232, RS-485 ali ekvivalentno).
- Rešitev mora omogočati konfiguracijo komunikacijskih parametrov za serijske vmesnike (npr. hitrost prenosa, pariteta, število bitov, stop bit) ter njihovo uporabo za sprejem in pošiljanje sporočil.
- Rešitev mora omogočati sočasno uporabo več različnih integracijskih metod znotraj iste implementacije.

2.3.1.9 Integracija z obstoječo SMS infrastrukturo

- Rešitev se mora integrirati z obstoječo SMS gateway napravo naročnika SMSEagle preko IP vmesnika.
- Integracija mora podpirati:
 - pošiljanje SMS sporočil,
 - sprejem SMS sporočil,
 - dvosmerno komunikacijo med sistemom in SMS gateway napravo.
- Rešitev mora omogočati uporabo standardnih IP komunikacijskih metod, kot so HTTP/HTTPS API ali enakovredni vmesniki, brez potrebe po zamenjavi obstoječe SMS infrastrukture.

2.3.1.10 Sočasna uporaba več kanalov

- Rešitev mora omogočati hkratno uporabo več vhodnih in izhodnih komunikacijskih kanalov, pri čemer morajo biti vsi kanali aktivni istočasno.
- Rešitev mora omogočati, da različni sistemi uporabljajo različne vhodne metode, ki se obdelujejo znotraj istega centralnega sistema.

2.3.1.11 Upravljanje in administracija

- Rešitev mora omogočati:
 - centralizirano upravljanje konfiguracije,
 - upravljanje komunikacijskih tokov in pravil,
 - upravljanje uporabnikov, skupin in prejemnikov,
 - pregled nad vsemi vhodnimi in izhodnimi sporočili,
 - sledljivost in revizijo komunikacije.
- Rešitev mora omogočati razširljivost z dodatnimi funkcionalnostmi ali integracijskimi moduli.

2.3.1.12 Arhitekturna zahteva

- Rešitev mora delovati kot centralni strežniški sistem za obdelavo sporočil, kjer se vsa vhodna sporočila iz različnih virov obravnavajo skozi enoten procesni mehanizem z lastnim življenjskim ciklom sporočila, trajno čakalno vrsto, možnostjo transformacije vsebine in dinamičnega usmerjanja na več izhodnih kanalov.

2.3.2 Podpora

Cena podpore mora biti vključena v skupno ceno ponujene rešitve in ne sme biti predmet dodatnega letnega ali periodičnega zaračunavanja.

Rešitev mora vključevati pravico do trajne (lifetime) podpore za celotno življenjsko dobo sistema, brez časovne omejitve veljavnosti podpore. Podpora mora biti zagotovljena na način, ki omogoča trajno uporabo rešitve z vsemi funkcionalnostmi tudi v primeru, da naročnik ne podaljša oz. naroči nobenih dodatnih storitev ali naročniških razmerij.

Podpora mora vključevati:

- dostop do tehnične podpore proizvajalca ali izvajalca,
- odpravo napak in tehnično pomoč,
- dostop do vseh prihodnjih posodobitev programske opreme,
- dostop do nadgradenj (minor in major verzije),
- dostop do varnostnih popravkov,
- dostop do dokumentacije in baze znanja.

Podpora mora omogočati neomejeno uporabo vseh posodobitev programske opreme brez dodatnih licenčnih stroškov.

Ponudnik mora zagotoviti, da za uporabo novih verzij programske opreme ni potrebno sklepanje dodatnih vzdrževalnih pogodb ali plačevanje dodatnih licenčnih stroškov.

2.3.3 Rok dobave

Rok dobave za ponujeno programsko opremo znaša 30 koledarskih dni po sklenitvi pogodbe.

2.4 Sklop 4: Kela CTI (podaljšanje licence)

Predmet sklopa 4 je podaljšanje licenc za obstoječo rešitev za kibernetško obveščevalno dejavnost (CTI), ki jo naročnik že uporablja v okviru svojih varnostno-operativnih procesov.

Podaljšanje licenc je potrebno za zagotavljanje neprekinjenega delovanja rešitve in ohranjanje ustreznih ravni kibernetške varnosti, ter skladnosti z veljavnimi zahtevami in standardi.

2.4.1 Zahteve za sklop 4

Postavka	Predmet	Zahteva
1	Nakup licence za 2 leti	KELA CTI - KEL-IDG modul; 25 Fully Qualified Domains 1 Playbook 12 months historical Data

Izbrani ponudnik bo za obdobje 24 mesecev zagotovil veljavne licence za uporabo platforme KELA CTI ter pripadajoče dostope do vseh funkcionalnosti in vsebin, ki jih platforma nudi v okviru naročene storitve.

Poleg zagotavljanja licenc bo ponudnik zagotavljal osnovno tehnično in administrativno podporo naročniku pri uporabi platforme, vključno z urejanjem dostopov, podporo pri konfiguraciji, ter posredovanjem zahtevkov do proizvajalca v primeru zaznanih težav ali potreb po dodatnih pojasnilih.

Ponudnik bo zagotavljal tudi, da ima naročnik v času trajanja pogodbe neprekinjen dostop do posodobitev in nadgradenj platforme, ki jih v okviru storitve zagotavlja proizvajalec, brez dodatnih vplivov na obstoječe podatke in delovanje sistema.

2.4.2 Dodatne zahteve za sklop 4

Ponudnik mora predložiti izjavo (angl. MAF) odgovorne osebe/proizvajalca ali uradnega zastopnika za območje Slovenije, da ima ponudnik s proizvajalcem ponujene opreme sklenjeno veljavno pogodbo, ki zajema tako dobavo opreme/licenc, kot tudi celotno podporo (dostop) do tehnične pomoči, dostop do baze znanj.

2.4.3 Rok dobave za sklop 4

Izvajalec mora dobaviti in aktivirati licence v roku 30 koledarskih dni po sklenitvi pogodbe.

Pogodbeni stranki ob dobavi in aktivaciji licenc podpišeta prevzemni zapisnik. Z dnem aktivacije licenc začne teči 24-mesečno obdobje za SKLOP 4, pri čemer se 24-mesečno obdobje zagotavljanja licenc in podpore šteje od dneva aktivacije licenc.

2.4.4 Tehnična podpora proizvajalca in odzivni čas za sklop 4

V času veljavnosti licenc, tj. v obdobju 24 mesecev, mora biti za naročnika zagotovljena Tehnična podpora proizvajalca z odzivnim časom v režimu 8x5 NBD (Next Business Day).

Za odzivni čas se šteje čas, v katerem proizvajalec potrdi od naročnika prejeto obvestilo o napaki.

..... *konec dokumenta*

