SPECIFIKACIJE

Obrazec P-5 »Specifikacije« je priloga kasneje sklenjene pogodbe.

Vrsta, lastnosti, kakovost in zgled predmeta javnega naročila/ponudbe

Predmet naročila	Enota	Celotna količina
Sklop 1: **Mobilne naprave / tablični računalniki / namenski zaboji za transport / sistem za enotno upravljanje s klienti** Vse ponujene naprave v tem sklopu morajo biti medsebojno popolnoma kompatibilne. Skladno s 7.alinejo, 2. odstavka, 6. člena **Uredbe o zelenem javnem naročanju (ZeJN)**, morajo tablični računalniki izpolnjevati okoljske zahteve na način, da imajo Energy Star cerftifikat. **Mobilne naprave / tablični računalniki** naprava naj ustreza zahtevam liste Android Enterprise Recommended za "Knowledge Workers Devices" (podrobnosti na spletni strani: https://www.android.com/enterprise/recommended/requirements/) in naj izpolnjuje vsaj naslednje minimalne zahteve: ○ Operacijski sistem: Android 9.0 ali novejši, ○ Pomnilnik vsaj: 2 GB ○ Prostor na disku minimalno: 32 GB ○ Hitrost procesorja vsaj: 1.4GHz ○ Delovanje na bateriji vsaj: 8ur ○ Ločljivost kamere (spredaj/zadaj) vsaj 2MP / 10MP ○ Arhitektura: 64bit ○ Zaslon 10 palcev ali večji ○ Poleg naj bo zagotovljen še zaščitni ovitek, izdelan posebej za ta model, z naslednjimi lastnostmi: ○ vključuje zaščito ekrana; ○ dodatna zaščita na robovih, da zagotavlja zaščito proti poškodbam ob padcih na tla; ○ zaščita proti prahu in praskam; ○ omogočen dostop do priključkov; ○ nemotena funkcija vseh tipk brez jemanja iz torbice/ovitka/zaščite. Ali ○ Tablica z operacijskim sistemom iOS z vsaj naslednjimi minimalnimi zahtevami: ○ Skladno s 7.alinejo, 2. odstavka, 6. člena **Uredbe o zelenem javnem naročanju (ZeJN)**, morajo tablični računalniki izpolnjevati okoljske zahteve na način, da imajo Energy Star cerftifikat. ○ Operacijski sistem: iOS 12 ali novejši ○ Prostor na disku minimalno: 32 GB ○ Delovanje na bateriji: 8h+ ○ Arhitektura: 64bit ○ Zaslon 10 palcev ali večji ○ Poleg naj bo zagotovljen še zaščitni ovitek, izdelan posebej za ta model, z naslednjimi lastnostmi: ○ vključuje zaščito ekrana; ○ dodatna zaščita na robovih, da zagotavlja zaščito proti poškodbam ob padcih na tla;	Kos	400

○ zaščita proti prahu in praskam; ○ omogočen dostop do priključkov; ○ nemotena funkcija vseh tipk brez jemanja iz torbice/ovitka/zaščite. Oprema mora podpirati upravljanje z mobilnostjo (Enterprise mobility management).		
Namenski zaboji za transport Za nemoteno ravnanje z mobilnimi napravami želimo namenske zaboje za transport, polnjenje in sinhronizacijo. Ti zaboji naj omogočajo, da so naprave med transportom varne pred fizičnimi poškodbami in sočasno skrbniku omogočajo lažji transport med lokacijami. Ponujeni kovčki morajo biti kompatibilni s ponujenimi mobilnimi napravami / tablicami. Prenosni polnilni kovčki naj izpolnjujejo vsaj naslednje osnovne zahteve: • v zaboj gre vsaj 10 naprav; • vse naprave se lahko polnijo hkrati; • vse naprave v kovčku se lahko hkrati sinhronizirajo; • naprave so v zaboju zaščitene pred vremenskimi vplivi in fizičnimi poškodbami; • zaboj je zasnovan kot kovček na kolesih za lažji transport, ima čvrsto ohišje, odporno na vodo in izvlečni ročaj; • možnost zaklepa in priklepa zaboja. • Notranjost: - mehko obloženi prostori za vsaj 10 palčne tablične računalnike;	kos	32
Sistem za enotno upravljanje s klienti Ponujen sistem mora biti kompatibilen s ponujenimi mobilnimi napravami – tablicami. Sistem za enotno upravljanje s klienti naj združuje vse potrebne funkcije za obvladovanje večjega števila raznolikih naprav na enem mestu (enotna konzola) in s poenotenim pristopom. Omogoča naj konfiguracijo, nadzor in upravljanje naprav različnih namembnosti (pametni telefon, tablica, terminal, PC, IoT naprave) in operacijskih sistemov (iOS, Android, Windows 10, macOS). Poenotiti in centralizirati želimo vpeljavo novih aplikacij, konfiguracij, posodobitev, profilov, varnostnih nastavitev (omejitev), preverjanja skladnosti in varovanja podatkov. Ponujena rešitev naj nudi enoten pregled na celoten ekosistem klientov in uporabnikov. S tem naj omogoča učinkovito podporo končnim uporabnikom ter zbiranje uporabnih informacij o sistemih in aplikacijah. Omogoča naj napredne rešitve za prijavo uporabnikov (identitete) in vzpostavitev varnih povezave do sredstev v internih omrežjih. Potrebne funkcionalnosti: Enostavna oziroma samodejna konfiguracija nove naprave (QR koda, samodejno preko serijske številke naprave vezane na stranko). IZHODIŠČE: Velikega števila naprav ni smiselno konfigurirati ročno, saj je to časovno potratno. Naprave se lahko od proizvajalca pošljejo direktno do uporabnikov. Ob vklopu in povezavi z omrežjem se naprava	Licenca / uporabnika	400

konfigurira samodejno glede na nastavljen način (serijska številka, QR koda,....itd.). **Zahteva**: Celovito upravljanje nastavitev naprave in aplikacij s strani lastnika. Uporabnik nima kontrole nad nameščanjem aplikacij, posodobitev in spreminjanjem nastavitev, ki jih skrbnik ne dovoljuje. IZHODIŠČE: Uporabnikom se prepreči spreminjanje nastavitev naprave in nameščanje poljubnih aplikacij. Vse aplikacije in nastavitev delegira skrbnik preko centralnega sistema. To je pomembno zaradi varnosti in enotnosti konfiguracije naprav. S tem se znatno zmanjša možnost pojava nepredvidljivih napak, nepooblaščenega odliva podatkov in širjenja zlonamerne kode. **Zahteva**: Blokada vseh nepotrebnih (ne odobrenih) aplikacij in storitev, ki jih naprava omogoča (kiosk način). IZHODIŠČE: Omejitev funkcij in aplikacij le na tiste, ki so potrebne za delovni proces. Mobilne naprave bodo med drugim uporabljali občani, ki niso del organizacije. Proces predvideva povezavo aplikacije v notranje ZNET omrežje, kar predstavlja varnostno tveganje. Z blokado vseh aplikacij, ki uporabnikom niso namenjene in jih ne potrebujejo pri željenem procesu, omejimo možnost povzročitve škode ali nepooblaščenega dostopa do podatkov. **Zahteva:** Upravljanje s certifikati in naprednimi politikami za dostop do omrežja. IZHODIŠČE: Centralno urejanje nastavitev mrežnih povezav na varen način. **Zahteva:** Upravljanje s posodobitvami naprave (firmware, operacijski sistem). IZHODIŠČE: Kontrolirano nameščanje posodobitev naprave tako, da je ta vedno tehnično in varnostno skladna. Posodobitve se tako lahko predhodno ustrezno testirajo. S tem zmanjšamo možnost napake na aplikaciji iz naslova nepooblaščene posodobitve naprave ali varnostnega incidenta zaradi varnostnih ranljivosti v primeru ne posodobljenih naprav. **Zahteva:** Upravljanje dostopov do vhodno/izhodnih vrat. IZHODIŠČE: Mobilne naprave bodo uporabljali občani, ki niso del organizacije. Proces predvideva povezavo aplikacije v notranje ZNET omrežje, kar predstavlja varnostno tveganje. Zahteva: Zaprejo se vhodno/izhodna vrata (usb, bralniki spominskih kartic,...itd.), kar preprečuje da bi uporabnik preko nepooblaščenega pomnilnega medija ali druge naprave spravil v omrežje ZNET zlonamerno kodo. Zahteva: Politika zaklepa zaslona. IZHODIŠČE: Preprečuje uporabo ob neprisotnosti pooblaščene osebe (brez vpisa gesla). **Zahteva:** Upravljanje z napravo (zaklepanje /odklepanje naprave, reset naprave, brisanje naprave).		

IZHODIŠČE: Odvzem/povrnitev dostopa do naprave iz strani upravitelja, menjava lastnika naprave (reset) ali izbris naprave v primeru kraje, izgube ali ukinitve upravljanja funkcije. **Zahteva:** Centralno upravljanje zaščite proti virusom in ostali zlonamerni kodi. Napredne VPN funkcionalnosti, ki omogočajo konfiguracijo obnašanja VPN povezav glede na uporabnika. IZHODIŠČE: Uporabnik se ne ukvarja s konceptom VPN povezave in mu je ta del skrit. Prijavljen uporabnik ima določena dovoljenja za uporabo aplikacij. VPN se vključi samodejno v ozadju in to le za promet dotične aplikacije (per-app VPN, always-on). Preostali promet gre mimo VPN povezave. Tak način močno zmanjša tveganje nepooblaščenega dostopa do podatkov v notranjem ZNET omrežju. V tem primeru VPN vzpostavlja vsaka naprava (aplikacija) posebej in to ni v domeni dostopne točke (vezano na točko 3.). Ponudba naj vključuje dobavo, zagon in osnovno nastavitev rešitve in nadgradnje na najnovejšo priporočeno različico programske opreme. Točen datum instalacije uskladita skrbnika pogodbe na strani naročnika in ponudnika. **Podrobnejše tehnične zahteve** Upravljanje naprave mora obsegati najmanj funkcije preverjanja in nastavitev skladnosti z varnostnimi pravili na področjih: 1) **Preverjanje skladnosti naprave**; zagotavlja skladnost tipa naprave, operacijskega sistema, število dovoljenih naprav, osnovnih varnostnih nastavitev in preprečevanje nepooblaščenega dostopa kot: a) načini razpoznavanja uporabnika, b) dolžina in kompleksnost gesel; c) avtomatizirano preverjanje in poročanje skladnosti: i) z osnovnimi varnostnimi pravili (rooted, jailberak, enkripcija) ii) nameščenih zahtevanih aplikacij (s stališča skladnosti naprave: odjemalec, protivirusna zaščita); d) omejevanje dostopa do posebnih funkcij ali storitev, na primer brskalnika, multimedijskih naprav ali komunikacijskih povezav (npr. Bluetooth ipd.); e) integracijo z digitalnimi potrdili (certifikati); za področja validacije uporabnika in naprave. Povezava storitev in funkcij naprave za veljavnosti digitalnega potrdila; f) avtomatska eskalacija v primeru neskladnosti (obveščanje, odstranitev, blokiranje, ..) 2) **Upravljanje dostopa**; pogojno upravlja funkcionalnost kot so npr.: dostop do portala z mehanizmi enotne prijave (SSO), več-faktorskim overjanjem, one-touch SSO, pogojni dostop in pogojni dostop na podlagi ocene tveganja. 3) **Omejitve uporabe**: a) pravilno in skladno varovanje zasebnosti uporabnika in uporabe, kot raven upravljalnega nadzora skrbnikov nad aktivirano napravo, podrobna opredelitev, katere podatke je mogoče videti ali spremljati, na sami upravljani napravi;		

b) zbiranja in obdelave podatkov na področju varovanja in v primeru preiskav zasebnosti. 4) **Omejitev uporabe aplikacij**: a) dostopnost aplikacij; obravnava pravil dostopa do varnostno skladnih aplikacij znotraj lastne trgovine notranjih, licenčnih in prostih aplikacij. 5) funkcionalne uporabe gradnikov in storitev sistema: a) registracijo in vključitev uporabnika, b) varno lokalno shrambo podatkov, c) varen dostop do dodeljenih aplikacij. Celovito upravljanje mora k pogojem delnega upravljanja zagotoviti še najmanj naslednje kategorije in njihove osnovne funkcionalnosti: 1) Celovito upravljanje in zagotavljanje naprave in vsebine; možnost izvedbe celovitega upravljanja naprave, vključno s strojno opremo, operacijskim sistemom, aplikacijami 2) Zagotavljanje varnih aplikacij in podatkovnega prenosa; upravljanje aplikacij za mobilne naprave (MAM) z DLP in vsebnikom SDK, nadzor nad namestitvijo in zagonom veljavnih aplikacij, kontejnerske aplikacije za mobilne naprave (e-pošta, brskalnik, vsebina, lokalna hramba), 3) Enotno upravljanje končnih točk; celovito upravljanje naprave in vsebine z možnostjo izvedbe celovitega upravljanja naprave, vključno s strojno opremo, operacijskim sistemom, upravljanje mobilnih naprav (MDM). Naročnik od ponujenega sistema/rešitve zahteva izpolnjevanje vseh v nadaljevanju navedenih funkcionalnosti: 1. Da principal rešitve izdaja nove verzije / dopolnitve sočasno (zero-day) z novimi verzijami programske opreme prenosnih naprav. 2. Zaradi varnosti podatkovnega toka naročnik izrecno zahteva da rešitev: a. podpira ločevanje gradnikov v različne segmente omrežja naročnika; b. podpira ločevanje gradnikov / funkcionalnosti najmanj na naslednje ločene elemente; i. upravljavska konzola – lokalno omrežje, ii. dostop za mobilne naprave – DMZ omrežje, iii. integracija z zalednimi sistemi (LDAP imenik, CA/CRL, SMTP obveščanje) – lokalno omrežje, iv. možnost ločevanja prometa po gradnikih rešitve glede na vsebino le tega najmanj za: elektronsko pošto, spletne vsebine notranjih spletnih strežnikov; c. Noben gradnik, ki se nahaja na podatkovni poti informacij med uporabnikom in zalednim sistemom, ne sme shranjevati podatkov, pač pa jih lahko le posreduje. d. Rešitev mora biti v celoti obvladljiva/upravljana s strani kompetentnega kadra naročnika. Noben od gradnikov rešitve ne sme biti upravljavsko nedostopen naročniku v smislu: i. Potrebe po privilegiranem upravljavskem dostopu za izvedbo poglobljenega vpogleda v delovanje ob identifikaciji ali odpravi napak. 3. Podprti OS prenosnih naprav končnih uporabnikov, od tega vsaj:		

a. pametni telefoni in tablični računalniki: i. Android 4.1 IN vsi novejši ii. Apple iOS 8+, IN vsi novejši iii. Chrome OS v39+; iv. Windows Phone 8+, Windows 10 Mobile v. Windows Mobile 5, 6.1, 6.5 b. delovne postaje: i. Windows 7, 8.1, 10 in ii. Apple Mac OS X 10.7 (Lion) in novejši; c. namenske naprave (rugged) za uporabo v zahtevnejših pogojih dela (popisne naprave, čitalci črtne kode, ipd.): i. Android verzije 3.0+, ii. Windows Mobile 5, 6 and 7 iii. Windows CE, CE x86 iv. Windows Embedeed 4. Podpora za deljene ali kiosk naprave; za vsa podprta okolja prenosnih naprav in neodvisno od proizvajalca strojne opreme mora biti podprta uvedba naprave v deljenem oziroma kiosk načinu, 5. Več-naročniška podpora; ponujena rešitev naj zagotovi enotno, iz središčne konzole enotno upravljano celovito več-naročniško podporo za najmanj: a. izgradnjo hierarhične, upravljavsko, aplikacijsko in varnostno ločene organizacijske strukture (starš – otrok), z možnostjo izbire dedovanja nastavitev ali izgradnje celovite nove strukture pravic in pooblastil v podrejenih ravneh, b. upravljanje več organizacijsko, upravljavsko ali lokacijsko medsebojno neodvisnih ali ločenih ravni, c. za vsako podrejeno raven popolnoma porazdeljeno (delegirano) upravljanje s hierarhično gradnjo pooblastil, pri čemer podrejeni del za izvajanje opravil administracije ne sme potrebovati korenskih ali pooblastil višje ravni, d. ločevanje profilov uporabnikov in skupin, e. podporo AD imenikom v organizaciji z več ravnimi (multi-tiered), f. gradnjo in upravljanje lastnega, lokalnega okolja uporabnikov. 6. Upravljanje identitet (IDM); rešitev mora zagotoviti središčni mehanizem, ki na osnovi razpoznavanja uporabnika, naprave in lokacije za mobilne, spletne, SaaS aplikacije zagotavlja: a. integracije (brez posrednika) s središčnim AD imenikom za centralizirano in polno sledenje upravljanja življenjskega cikla uporabnika: prihod, spremembe, odhod; b. nadzora uporabniškega dostopa na osnovi pripadnosti skupinam: i. definirane metode različnih metod overjanja (npr.: LDAP, RSA, RADIUS) po skupinah uporabnikov znotraj enega središčnega imenika. ii. Ločen omrežni dostop za poslovne (npr. katerokoli omrežje) in zunanje uporabnike (samo določeno omrežje); iii. selektivni / pogojni aplikacijski dostop za mobilne, spletne in Windows aplikacije. c. granulacijo varnostnih mehanizmov upravljanja identitet, transporta in selektivnega dostopa do aplikacij in vsebin		

kot funkcije: tipa naprave aplikacije, uporabnika, lokacije naprave; d. Mehanizme nadzora pogojnega dostopa (conditional-access), e. Polno licenčno pokritost celotne funkcionalnosti za vse uporabnike; 7. Mehanizem več-faktorskega overjanja (MFA) s podporo: a. Uporabe lastnega potisnega mehanizma razdeljevanja žetonov; b. Zagotavlja aplikacijo za generacijo žetonov v primeru delovanja brez povezave; c. Razdeljuje žetone preko kratkih (SMS) sporočil; d. Zagotavlja enotni aplikacijski katalog tudi v primeru integracije z zunanjimi sistemi MFA; 8. Sistem enkratne prijave (SSO); mora zagotoviti mehanizme varne, enotne prijave tudi za tiste naročnikove informacijske sisteme (storitve, aplikacije), ki podpirajo metode overjanja ali vmesnike, ki niso integrirani v središčni AD imenik. Sistem mora podpirati različne: a. Vhodne : AD uporabniško ime in geslo, iOS Kerberos, Radius, RSA SecurId, RSA Adaptive Auth, OAuth2, Android Cert., Kerberos, Digitalno potrdilo, SAML, b. izhodne : SAML, spletne servise (WS-*), Password Vault, Kerberos mehanizme overjanja. 9. Spremljanje in upravljanje inventorija prenosnih naprav, zagotavlja: a. središčno upravljanem z inventorijem strojne in vse podprte programske opreme b. vpogled za pooblaščene uporabnike v realnem času v inventorij strojne in programske opreme c. evidentiranje podatkov: i. napravi (podatki o strojni in programski opremi) in lastništvu ii. o operaterju, povezavah (podatkovna, govorna, Wi-Fi), gostovanju iii. o stanju povezave v rešitev (datum zagona, zadnjič videna, d. pred pripravljena poročila ali možnost gradnje poročil. MDM (Upravljanje mobilnih naprav) 1. Združljivost a. Vse funkcionalnosti navedene v nadaljevanju so razpoložljive na vseh zahtevanih podprtih operacijskih sistemih. 2. Integracija: a. Microsoft Exchange; b. Active Directory / LDAP; c. ActiveSync; d. Samsung SAFE; e. Samsung KNOX; 3. Varnostne značilnosti: a. Zaščita / ponastavitev gesla (Password protection/reset); b. Oddaljeno brisanje (Remote wipe); c. Daljinsko zaklepanje (Remote lock);		

d. Pridobitev privilegiranega nadzora (Jailbreak, rooted detection); e. Konfiguracija omrežij WiFi (Configure/disable WiFi); f. Konfiguracija VPN / Proxy / Gateway (Configure VPN/Proxy/Gateway); g. Šifriranje naprave (Device Encryption); h. Enotna prijava (Single Sign-On (SSO)); i. Upravljanje Identitet (Identity Management); j. Ločevanje uporabniških in poslovnih podatkov (Separate User from Corporate Data); k. Posodobitve operacijskega sistema (OS Updates); l. Upravljanje funkcionalnosti vgrajene opreme ali sistemske funkcionalnosti, v odvisnosti od lokacije naprave (Location-aware system function); rešitev mora podpirati različne ravni, omogočanja / onemogočanja ali pravil zagona sistemskih virov (vse vrste komunikacije, kamera, …) v odvisnosti od lokacije kjer se naprava nahaja ali od kje vzpostavlja podatkovno komunikacijo; 4. Sistemsko upravljanje in poročanje: a. Spletna skrbniška konzola (Web-based admin console) b. Integracija zunanjega upravljanja (API, ipd.) (3rd party management integration) c. Analitika na ravni naprave (Device-level analytics) d. Nadzorna plošča v realnem času (Real-time dashboard) e. Opozorila (Alerts) MAM (Upravljanje mobilnih aplikacij) 1. Združljivost; vse funkcionalnosti navedene v nadaljevanju morajo biti razpoložljive na vseh zahtevanih podprtih operacijskih sistemih. 2. Za potrebe razvoja varnih (razpoznavanje, transport, enkripcija hranjenih podatkov) internih mobilnih aplikacij uporabo namenskega razvojnega okolja in knjižnic (SDK) in funkcionalnosti ovijanja aplikacij (APP wrapping); 3. Preko namenske aplikacijske trgovine in/ali uporabniškega okolja uporabnikom omogočiti dostop do preverjenih, varnih in poslovno odobrenih: a. notranje razvitih aplikacij, b. poslovnih aplikacij tretjih oseb, 4. Zagotavlja aplikacij na ravni uporabnika in njegove naprave: a. personaliziran aplikacijski katalog, b. ločevanje deljenja podatkov med poslovnimi in privatnimi aplikacijami, 5. Zaščito integritete uporabnikovih osebnih podatkov (lokacija, neposlovna vsebina). 6. Varnostne značilnosti: a. Podpora delovanju aplikacij v kontejnerskem načinu (App Containerization) b. Evidenca dovoljenih / prepovedanih aplikacij (App whitelisting / blacklisting) c. Onemogoči kopiraj / prilepi v aplikacijah (Disable copy / paste in apps) d. Inventurno sledenje aplikacijam (App inventory tracking) e. Sledenje skladnosti aplikacij (App compliance tracking) f. Upravljanje različic aplikacij (App version management)		

g. Upravljanje konfiguracije aplikacij (App config mgmt) h. Nadzor dostopa na ravni uporabnikov in skupin (User & grp access control) i. Slednje največjega časa brez povezave (Maximum Offline Hours) j. Zahtevana poslovna raven preverjanja prijave (Required Enterprise Logon) k. Brisanje aplikacijskih podatkov ob zaklepanju (Erase App Data on Lock) 7. Sistemsko upravljanje in poročanje: a. Spletna skrbniška konzola (Web-based admin console) b. Potisne storitve (Push services) **Zahtevana strežniška infrastruktura ter arhitektura rešitve** Izvajalec mora v sklopu implementacije ponujene rešitve zagotoviti vse potrebne licence, ki jih potrebuje za uspešno implementacijo ponujene rešitve. Strežniško virtualno infrastrukturo zagotovi naročnik. Izvajalec mora ob oddaji ponudbe navesti sistemske vire, ki jih potrebuje za uspešno implementacijo rešitve. **Integracija v naročnikovo IKT okolje** Ponudnik mora izpolniti vse navedene zahteve in funkcionalnosti integracije v naročnikovo IKT okolje in sicer: 1. celovita integracija rešitve z gradniki IKT sistema potrebnimi za delovanje ponujene rešitve naročnika; 2. namestitev in konfiguracija ponujene rešitve; 3. konfiguracija 10 ponujenih mobilnih naprav (vzorčnih); 4. konfiguracija varnostne politike, profilov; 5. uvoz in konfiguracija uporabnikov; 6. spremljanje in konfiguracija delovanja; 7. izobraževanje naročnikovega uporabnika za samostojno upravljanje implementirane rešitve vključno s predajo uporabniške in tehniške dokumentacije. Navedene aktivnosti integracije morajo biti izvedene najkasneje v 10 dneh po dobavi opreme.		
Sklop 2: **Mobilne dostopne točke** Obstoječa naročnikova komunikacijska oprema v okviru zNet omrežja temelji na opremi proizvajalca Cisco Systems, za katero ima naročnik zagotovljene strokovnjake. V okolju je večina mrežne opreme proizvajalca Cisco Systems zato želimo zagotoviti kompatibilnosti z obstoječo komunikacijsko opremo proizvajalca Cisco Systems, Inc. Pričakujemo vsaj: • združljivost na funkcionalnem in protokolnem tehničnem nivoju z opremo obstoječega komunikacijskega omrežja zNET; • zanesljivo obratovanje v obstoječem sistemu oziroma omrežju; Osnovne ZAHTEVE Ponujena oprema mora biti namenjena slovenskemu trgu - torej takšna, da jo bo mogoče brez modifikacij uporabljati v Sloveniji ter jo v Sloveniji tudi vzdrževati. Dobavljena oprema mora biti opremljena z vsemi potrebnimi v Republiki Sloveniji veljavnimi atesti in dovoljenji za uporabo.	32	kos

1) Minimalne tehnične zahteve Splošne zahteve za strojno opremo: • samostoječa izvedba, z maksimalnimi dimenzijami 250mmX200mmX50mm; • usmerjevalnik mora biti primeren za najmanj 20 uporabnikov; • integrirana požarna pregrada (stateful firewall) z IPsec VPN in NAT; • možnost segmentacije omrežja z Vlan-i; • statično usmerjanje; • integriran DHCP strežnik; • samodejno posodabljanje; • možnost dodajanja funkcionalnosti IPS in blokiranja komunikacij glede na vsebino (content filtering); • vse zahtevane funkcionalnosti morajo biti na eni napravi. Performančne zmogljivost: • prepustnost požarne pregrade (stateful firewall) vsaj 80 Mbit/s prometa; • prepustnost vsaj 80 Mbit/s v tunelih IPsec VPN; • podpirati mora vsaj 10 hkratnih IPsec VPN tunelov. Vmesniki mrežne opreme: o vgrajenih najmanj 2 vmesnika 1000Base-Tx za LAN; o vgrajena najmanj 2 vmesnika za WAN; o vgrajen LTE modem CAT6. Brezžična funkcionalnost: • podpora 5GHz in 2,4GHz omrežja oz. standardov 802.11a/n/ac in 802.11b/g/n; • podpora avtentikacije WPA2-PSK; WPA2-Enterprise z 802.1X. Upravljanje naprav: • grafično upravljanje in nastavljanje naprav preko namenske, centralne, spletne aplikacije (protokol https) v javnem internetnem oblaku; • prikaz obremenitev naprav; • prikaz prepustnosti in stanja naprav z alarmiranjem; • prikaz in nadzor delovanja VPN tunelov.		
Sklop 3: **Strežnik** Infrastruktura za eZdravje je implementirana na HPE strojni opremi tako na strežniškem kot na shranjevalnem (storage) delu. Naslednji ekvivalenten ali zmogljivejši rezinski (blade) strežnik želimo vgraditi v obstoječo HPE rezinsko (blade) šasijo: Količina Opis 1 HPE ProLiant BL460c Gen10 10Gb/20Gb FlexibleLOM Configure-to-order Blade 1 HPE BL460c Gen10 Intel **Xeon-Silver** 4 HPE 16GB (1x16GB) Single Rank x4 DDR4-2666 CAS-19-19-19 Registered Sm 4 Factory Integrated	kos	1

2	HPE 600GB SAS 12G Enterprise 10K SFF (2.5in) SC 3yr Wty Digitally Signed Firmware HDD ali ustrezen SS		
2	Factory Integrated		
1	HPE 12W Smart Storage Battery (up to 3 Devices) for BladeSystem Server		
1	Factory Integrated		
1	HPE Smart Array P204i-b SR Gen10 (4 Internal Lanes/1GB Cache) 12G SAS Modular Controller		
1	Factory Integrated		
1	HPE FlexFabric 10Gb 2-port 536FLB Adapter Factory Integrated		
	Ali ekvivalenten produkt.		
Sklop 4: **Oracle licence** Komplet: Oracle Database Processor Perpetual, 4 CPU jedra Diagnostic Pack Processor Perpetual, 4 CPU jedra Tuning Pack Processor Perpetual, 4 CPU jedra SOFTWARE UPDATE LICENSE & SUPPORT		Št. licenc	 2 2 2 1

Garancija in čas popravila:
Garancija vsaj eno leto.
Ponudnik se zaveže, da bo odzivni čas za vse napake na strojni opremi v obdobju vsaj eno leto na lokaciji kupca (NIJZ in P-5a_seznam izbranih ZD z naslovi.xls) največ naslednji delovni dan. Za odzivni čas se šteje dejanski čas, ki preteče od trenutka, ko kupec javi napako in ponudnikovim pričetkom odprave te napake. Ponudnik opreme se obvezuje:

- odpraviti prijavljeno okvaro na nedelujoči opremi najkasneje v roku naslednjega delovnega dne oziroma jo zamenjati z enako opremo ali njenim funkcionalnim ekvivalentom od trenutka predaje nedelujoče opreme v popravilo ponudniku (osebna dostava ali po pošti) na lokaciji ponudnikovega servisa;
- brezplačno zagotavljati vse nove verzije programske opreme v okviru iste funkcionalnosti;
- zagotavljati rezervne dele za vso dobavljeno opremo.

Garancijski rok za programsko opremo mora biti vsaj 12 mesecev.

Druge zahteve
Ponudba mora vsebovati vse predvidene stroške povezane z dobavo opreme. Ob dostavi se naročniku v elektronski obliki dostavi seznam opreme s serijskimi številkami posameznih kosov.

Ponudba mora vsebovati natančne navedbe modelov ponujene opreme – naziv proizvajalca in modelno številko oziroma druge komercialne oznake ponujene opreme, iz katerih je možno nedvoumno razbrati tehnične lastnosti posamezne ponujene opreme.

Dobavni rok: največ 21 dni.

Oprema, ki se dobavi mora:

- biti nova, iz tekoče proizvodnje in narejena iz standardnih prvorazrednih materialov.
- imeti lastnosti, ki ustrezajo proizvajalčevemu atestu, tehnični dokumentaciji in navodilom za uporabo.
- biti izdelana skladno z zakonodajo o varstvu pri delu v Republiki Sloveniji.

Opomba: Vsa imena registriranih ali zaščitenih proizvodov, blagovnih znamk in imena podjetij uporabljena v tej razpisni dokumentaciji so blagovne znamke ali registrirane blagovne znamke njihovih lastnikov.

Spodaj podpisani pooblaščeni predstavnik ponudnika izjavljam, da vse ponujeno blago v celoti ustreza zgoraj navedenim opisom.

V/na _____, dne _____

Ime in priimek:

Žig in podpis: