# Izmjena postupka

**OSNOVNI PODACI**

Opis predmeta javne nabavke:

Održavanje aplikacija i sistema baziranih na OpenSource tehnologijama

Vrsta predmeta:

Usluge

Vrsta postupka:

Otvoreni postupak

**PODACI O NARUČIOCU**

Naziv:

FOND ZA ZDRAVSTVENO OSIGURANJE

PIB:

02010810

## Uslovi prije izmjena

| Opis | Tip uslova |
| --- | --- |
| U postupku javne nabavke može da učestvuje samo privredni subjekat koji: 1) nije pravosnažno osuđivan i čiji izvršni direktor nije pravosnažno osuđivan za neko od krivičnih djela sa obilježjima: a) kriminalnog udruživanja; b) stvaranja kriminalne organizacije; c) davanje mita; č) primanje mita; ć) davanje mita u privrednom poslovanju; d) primanje mita u privrednom poslovanju; dž) utaja poreza i doprinosa; đ) prevare; e) terorizma; f) finansiranja terorizma; g) terorističkog udruživanja; h) učestovanja u stranim oružanim formacijama; i) pranja novca; j) trgovine ljudima; k) trgovine maloljetnim licima radi usvojenja; l) zasnivanja ropskog odnosa i prevoza lica u ropskom odnosu što se dokazuje na osnovu uvjerenja, potvrde ili drugog akta nadležnog organa izdatog na osnovu kaznene evidencije, u skladu sa propisima države u kojoj privredni subjekat ima sjedište, odnosno u kojoj ovlašćeno lice tog privrednog subjekta ima prebivalište. | Obavezni uslovi |
| U postupku javne nabavke može da učestvuje samo privredni subjekat koji je izmirio sve dospjele obaveze po osnovu poreza i doprinosa za penzijsko i zdravstveno osiguranje, o kojima evidenciju vodi organ uprave nadležan za naplatu poreskih prihoda, odnosno nadležni organ države u kojoj privredni subjekat ima sjedište. Ispunjenost obaveznih uslova dokazuje se na osnovu uvjerenja, potvrde ili drugog akta koji izdaje organ uprave nadležan za naplatu poreskih prihoda, odnosno nadležni organ države u kojoj privredni subjekat ima sjedište. | Obavezni uslovi |
| Izjava privrednog subjekta verifikovana elektronskim potpisom (ponuđač mora popuniti i sačini izjavu privrednog subjekta u svemu prema UPUTSTVU za popunjavanje izjave, u skladu sa Pravilnikom o obrascu Izjave privrednog subjekta Sl.CG 55/23, 83/23). | ESPD |
| Rok važenja ponude je 60 dana od dana otvaranja ponuda. | Rok važenja ponude |
| Ponuđač je dužan dostaviti bezuslovnu i na prvi poziv naplativu garanciju ponude u iznosu od 2% procijenjene vrijednosti javne nabavke, kao garanciju ostajanja u obavezi prema ponudi u periodu važenja ponude i 8 dana nakon isteka važenja ponude | Garancija ponude |

| | |
|---|---|
| Mjesto izvršenja ugovora je: Fond za zdravstveno osiguranje Crne Gore, ul Vaka Đurovića bb, Podgorica (server sala i prostorija za siguran pristup sistemu). | Mjesto izvršenja ugovora |
| Rok plaćanja: 30 dana od dana uredno dostavljene mjesečne fakture. | Rok plaćanja |
| Način plaćanja je: Virmanski | Način plaćanja |
| Primopredaja i puštanje u rad: Primopredaja i puštanje u rad aplikacija i sistema koji su predmet nabavke je 3 dana od dana zaključivanja ugovora | Primopredaja i puštanje u rad |
| Uslovi za primopredaju: Realizovana implementacija u produkcionom okruženju mora da omogućava funkcionalnosti u skladu sa opisima iz tehničkih zahtjeva što se isključivo utvrđuje od strane stručnog osoblja naručioca u roku ne dužem od jednog dana. | Uslovi za primopredaju |
| Rok izvršenja ugovora je godinu dana (12 mjeseci) od dana zaključivanja ugovora. Izvršilac će otpočeti sa uslugama tehničke podrške i održavanja aplikacija i sistema baziranih na OpenSource tehnologijama odmah nakon izvršene implementacije | Rok izvršenja ugovora |
| Ponuđač je u obavezi da dostavi spisak angažovanih stručnih lica sa navedenim poslovima na kojima će biti angažovani u realizaciji usluga koje su predmet javne nabavke. | Drugi uslovi |
| Privredni subjekat je dužan da posjeduje: - minimum iskustva na kvalitetnom i uspješnom izvršavanju istih ili sličnih poslova iz oblasti predmeta nabavke; -minimum 1 (jedna) potvrda o kvalitetnom i uspješnom izvršavanju istih ili sličnih poslova iz oblasti predmeta nabavke pruženih tokom prethodnih 5 godina, računajući i godinu u kojoj je započet postupak javne nabavke koje sadrže opis i vrijednost predmeta nabavke, vrijeme realizacije ugovora i konstataciju da je ugovor blagovremeno i kvalitetno izvršen.<br>Navedeno se dokazuje: -potvrdama izdatim od strane investitora, odnosno korisnika o pruženim uslugama tokom prethodnih godina ali ne duže od pet godina, računajući i godinu u kojoj je započet postupak javne nabavke, koje sadrže opis (iz kojeg se može zaključiti da se usluge odnose na poslovne i medicinske procese i o korišćenim softverskim razvojnim alatima) i vrijednost predmeta nabavke, broj korisnika, vrijeme realizacije ugovora i konstataciju da je ugovor blagovremeno i | Stručna i tehnička sposobnost |

kvalitetno izvršen . Isti ili slični poslovi na koje se potvrda mora odnositi su: implementaciju, održavanje i tehničku podršku za sisteme bazirane na OpenSource tehnologijama sa sljedećim karakteristikama: - Firewall/Ruter klaster u active/backup ili active/active režimu rada u 40Gbps mrežnom okruženju koji opslužuje minimum 300 mrežnih entiteta i minimum 80 vlan mreženih segmenata; - VPN koncentrator koji opslužuje minimum 40 udaljenih lokacija sa identifikacijom lokacija po modelu klijentskih x509 sertifikata i provjerom validnosti sertifikata preko OCSP protokola; - SSL/TLS gateway za HTTP saobraćaj sa dvo-faktornom autentifikacijom pristupa i sa administratorskim interfejsom; - Virtuelizacija servera bazirana na KVM tehnologiji sa klasterizovanim OCFSv2 fajl sistemom i SDS storage sistemom za smještanje disk image-a od virtuelnih mašina, sa implementiranim funkcionalnostima (neosjetno za rad virtuelne mašine) uživo migracija virtuelnih mašina (live migration) i uživo backup diska virtuelnih mašina (live snapshot), uživo migracija cijelog jednog hipervizora na drugi, implementacija koja opslužuje minimum 70 virtuelnih mašina; - Mail sistem, sa webmail interfejsom, sa antispam i antivirus zaštitom, dkim i dmarc mehanizmima, imap protokol, klase kvaliteta servisa za korisnike (max broj mejlova, veličina poruke, broj primalaca u jedinici vremena), centralizovano upravljanje autorizacijom, koji opslužuje minimum 80 korisnika; - Sistem za mrežni monitoring preko kojeg se prati minimum 15 entiteta; - Proxy sistem koji opslužuje minimum 80 korisnika; - DNS sistem sa master serverom na jednoj i slave serverom na drugoj udaljenoj lokaciji; - VPN klijentsko rješenje sa Linux ruterom koje se koristi na minimum 10 udaljenih lokacija; - SMS gateway sa godišnjim prometom minimum 180000 SMS poruka i sa API autentifikacijom za slanje poruka; - SSO (Single Sign-on) sistem za siguran pristup i administraciju Linux servera, sa identifikacijom administratora pomoću username/passworda po principu SSO (administratoru se odobrava pristup do servera, preko SSH ili drugog mehanizma, bez ponovne autentifikacije passwordom), po administratoru personalizovani mrežni direktorijum koji je dostupan sa svih ulogovanih servera, implementacija za administriranje minimum 20 Linux servera; - HTTPS gateway sa algoritamskim balansiranjem saobraćaja, sa

| | |
|---|---|
| autentifikacijom udaljenih klijenata prije balansiranja dolaznog saobraćaja po modelu username/password ili klijentskih x509 sertifikata, balansiranje dolaznog saobraćaja prema unutrašnjim URL putanjama uz opciju ‘sticky’ sesije (na način da svi narednih zahtjevi se šalju ka onoj untrašnjoj putanji na koju je prvo preusmjerena dolazna konekcija), monitoring ispravnosti unutrašnjih URL putanja, implementacija koja opslužuje minimum 300 udaljenih klijenata; - Crypto sistem, CA funkcionalnost sa OCSP endpoint-om, AES-GCM algoritam i AES256 ključevi za kriptografiju, PKCS11 interfejs prema HSM modulu, hijerarhija ključeva za potrebe korisničkih kriptografskih operacija koja ne zahtjeva upotrebu HSM modula nakon urednog starta/učitavanja sistema, korisnički API servisi za kriptografske operacije, rotiranje simetričnih ključeva, upravljački interfejs koji podržava proizvoljne logičke kombinacije uslova filtera za pretragu ključnih entiteta uz eksport podataka u Excel fajlove, API interfejs za integraciju sa drugim sistemima, samostalni alati za oporavak/dekripciju podataka u offline režimu rada u slučaju da nije moguće oporaviti API servis za kriptografske operacije. - Backup 3-2-1 sistem, koji se bazira na tri nezavisne implementacije smještanja podataka, od kojih dvije moraju biti SDS storage implementacije, od čega se na dvije implementacije podaci smještaju na različitim medijumima (mehanički, ssd diskovi i sl.), od čega minimum treća implementacija mora biti fizički/prostorno izdvojena u odnosu na druge dvije i koja u predviđeno vrijeme isključivo jednostrano inicira prenos podataka. | |

| | |
|---|---|
| Privredni subjekat je dužan da posjeduje: minimum stručnih i kadrovskih kapaciteta koji su potrebni za izvršenje ugovora: - Minimum 1 stručno specijalizovano lice (koje će biti angažovano na realizaciji predmeta nabavke tokom cijelog ugovorenog perioda) za pružanje usluga implementacije, održavanja i tehničke podrške, koje posjeduje važeći sertifikat u rangu Linux-inženjera, sertifikat specijalizacije za SDS storage sistem, sertifikat specijalizacije za Virtuelizaciju i sertifikat specijalizacije za Visoko-dostupne klastere, kao ličnu referencu stručne i tehničke sposobnosti, pri čemu sertifikati moraju biti zasnovani po modelu izvršavanja konkretnih zadataka u realnom sistemskom okruženju (RHCE + RHCS sertifikat ili ekvivalent).<br>Navedeno se dokazuje dokazom o angažovanju radne snage i dokazom o stručnoj osposobljenosti , i to: - dokazi o angažovanju radne snage (prijava na osiguranje zaposlenog, ugovor o radu, sporazum o preuzimanju zaposlenog, ugovor o korišćenju sposobnosti drugog subjekta ili drugi akt u skladu sa zakonom), - dokaz o stručnoj osposobljenosti (sertifikat, uvjerenje ili drugi akt nadležnog organa ili organizacije). | Stručna i tehnička sposobnost |

**Uslovi nakon izmjena**

| Opis | Tip uslova |
|---|---|
| U postupku javne nabavke može da učestvuje samo privredni subjekat koji: 1) nije pravosnažno osuđivan i čiji izvršni direktor nije pravosnažno osuđivan za neko od krivičnih djela sa obilježjima: a) kriminalnog udruživanja; b) stvaranja kriminalne organizacije; c) davanje mita; č) primanje mita; ć) davanje mita u privrednom poslovanju; d) primanje mita u privrednom poslovanju; dž) utaja poreza i doprinosa; đ) prevare; e) terorizma; f) finansiranja terorizma; g) terorističkog udruživanja; h) učestovanja u stranim oružanim formacijama; i) pranja novca; j) trgovine ljudima; k) trgovine maloljetnim licima radi usvojenja; l) zasnivanja ropskog odnosa i prevoza lica u ropskom odnosu što se dokazuje na osnovu uvjerenja, potvrde ili drugog akta nadležnog organa izdatog na osnovu kaznene evidencije, u skladu sa propisima države u kojoj privredni subjekat ima sjedište, odnosno u kojoj ovlašćeno lice tog privrednog subjekta ima prebivalište. | Obavezni uslovi |

| | |
|---|---|
| U postupku javne nabavke može da učestvuje samo privredni subjekat koji je izmirio sve dospjele obaveze po osnovu poreza i doprinosa za penzijsko i zdravstveno osiguranje, o kojima evidenciju vodi organ uprave nadležan za naplatu poreskih prihoda, odnosno nadležni organ države u kojoj privredni subjekat ima sjedište. Ispunjenost obaveznih uslova dokazuje se na osnovu uvjerenja, potvrde ili drugog akta koji izdaje organ uprave nadležan za naplatu poreskih prihoda, odnosno nadležni organ države u kojoj privredni subjekat ima sjedište. | Obavezni uslovi |
| Izjava privrednog subjekta verifikovana elektronskim potpisom (ponuđač mora popuniti i sačini izjavu privrednog subjekta u svemu prema UPUTSTVU za popunjavanje izjave, u skladu sa Pravilnikom o obrascu Izjave privrednog subjekta Sl.CG 55/23, 83/23). | ESPD |
| Rok važenja ponude je 60 dana od dana otvaranja ponuda. | Rok važenja ponude |
| Ponuđač je dužan dostaviti bezuslovnu i na prvi poziv naplativu garanciju ponude u iznosu od 2% procijenjene vrijednosti javne nabavke, kao garanciju ostajanja u obavezi prema ponudi u periodu važenja ponude i 8 dana nakon isteka važenja ponude | Garancija ponude |
| Mjesto izvršenja ugovora je: Fond za zdravstveno osiguranje Crne Gore, ul Vaka Đurovića bb, Podgorica (server sala i prostorija za siguran pristup sistemu). | Mjesto izvršenja ugovora |
| Rok plaćanja: 30 dana od dana uredno dostavljene mjesečne fakture. | Rok plaćanja |
| Način plaćanja je: Virmanski | Način plaćanja |
| Primopredaja i puštanje u rad: Primopredaja i puštanje u rad aplikacija i sistema koji su predmet nabavke je 3 dana od dana zaključivanja ugovora | Primopredaja i puštanje u rad |
| Uslovi za primopredaju: Realizovana implementacija u produkcionom okruženju mora da omogućava funkcionalnosti u skladu sa opisima iz tehničkih zahtjeva što se isključivo utvrđuje od strane stručnog osoblja naručioca u roku ne dužem od jednog dana. | Uslovi za primopredaju |
| Rok izvršenja ugovora je godinu dana (12 mjeseci) od dana zaključivanja ugovora. Izvršilac će otpočeti sa uslugama tehničke podrške i održavanja aplikacija i sistema baziranih na OpenSource tehnologijama odmah nakon izvršene implementacije | Rok izvršenja ugovora |

| | |
|---|---|
| Ponuđač je u obavezi da dostavi spisak angažovanih stručnih lica sa navedenim poslovima na kojima će biti angažovani u realizaciji usluga koje su predmet javne nabavke. | Drugi uslovi |
| Privredni subjekat je dužan da posjeduje: - minimum iskustva na kvalitetnom i uspješnom izvršavanju istih ili sličnih poslova iz oblasti predmeta nabavke; -minimum 1 (jedna) potvrda o kvalitetnom i uspješnom izvršavanju istih ili sličnih poslova iz oblasti predmeta nabavke pruženih tokom prethodnih 5 godina, računajući i godinu u kojoj je započet postupak javne nabavke koje sadrže opis i vrijednost predmeta nabavke, vrijeme realizacije ugovora i konstataciju da je ugovor blagovremeno i kvalitetno izvršen. Navedeno se dokazuje: - potvrdom/potvrdama izdatim od strane investitora, odnosno korisnika o pruženim uslugama tokom prethodnih godina ali ne duže od pet godina, računajući i godinu u kojoj je započet postupak javne nabavke, koje sadrže opis i vrijednost predmeta nabavke, vrijeme realizacije ugovora i konstataciju da je ugovor blagovremeno i kvalitetno izvršen . Isti ili slični poslovi na koje se potvrda mora odnositi su: implementaciju, održavanje i tehničku podršku za sisteme bazirane na OpenSource tehnologijama sa sljedećim karakteristikama: - Firewall/Ruter klaster u active/backup ili active/active režimu rada u 40Gbps mrežnom okruženju koji opslužuje minimum 300 mrežnih entiteta i minimum 80 vlan mreženih segmenata; - VPN koncentrator koji opslužuje minimum 40 udaljenih lokacija sa identifikacijom lokacija po modelu klijentskih x509 sertifikata i provjerom validnosti sertifikata preko OCSP protokola; - SSL/TLS gateway za HTTP saobraćaj sa dvo-faktornom autentifikacijom pristupa i sa administratorskim interfejsom; - Virtuelizacija servera bazirana na KVM tehnologiji sa klasterizovanim OCFSv2 fajl sistemom i SDS storage sistemom za smještanje disk image-a od virtuelnih mašina, sa implementiranim funkcionalnostima (neosjetno za rad virtuelne mašine) uživo migracija virtuelnih mašina (live migration) i uživo backup diska virtuelnih mašina (live snapshot), uživo migracija cijelog jednog hipervizora na drugi, implementacija koja opslužuje minimum 70 virtuelnih mašina; - Mail sistem, sa webmail interfejsom, sa antispam i antivirus zaštitom, dkim i dmarc mehanizmima, imap protokol, klase kvaliteta servisa za korisnike (max | Stručna i tehnička sposobnost |

broj mejlova, veličina poruke, broj primalaca u jedinici vremena), centralizovano upravljanje autorizacijom, koji opslužuje minimum 80 korisnika; - Sistem za mrežni monitoring preko kojeg se prati minimum 15 entiteta; - Proxy sistem koji opslužuje minimum 80 korisnika; - DNS sistem sa master serverom na jednoj i slave serverom na drugoj udaljenoj lokaciji; - VPN klijentsko rješenje sa Linux ruterom koje se koristi na minimum 10 udaljenih lokacija; - SMS gateway sa godišnjim prometom minimum 180000 SMS poruka i sa API autentifikacijom za slanje poruka; - SSO (Single Sign-on) sistem za siguran pristup i administraciju Linux servera, sa identifikacijom administratora pomoću username/passworda po principu SSO (administratoru se odobrava pristup do servera, preko SSH ili drugog mehanizma, bez ponovne autentifikacije passwordom), po administratoru personalizovani mrežni direktorijum koji je dostupan sa svih ulogovanih servera, implementacija za administriranje minimum 20 Linux servera; - HTTPS gateway sa algoritamskim balansiranjem saobraćaja, sa autentifikacijom udaljenih klijenata prije balansiranja dolaznog saobraćaja po modelu username/password ili klijentskih x509 sertifikata, balansiranje dolaznog saobraćaja prema unutrašnjim URL putanjama uz opciju ‘sticky’ sesije (na način da svi narednih zahtjevi se šalju ka onoj untrašnjoj putanji na koju je prvo preusmjerena dolazna konekcija), monitoring ispravnosti unutrašnjih URL putanja, implementacija koja opslužuje minimum 300 udaljenih klijenata; - Crypto sistem, CA funkcionalnost sa OCSP endpoint-om, AES-GCM algoritam i AES256 ključevi za kriptografiju, PKCS11 interfejs prema HSM modulu, hijerarhija ključeva za potrebe korisničkih kriptografskih operacija koja ne zahtjeva upotrebu HSM modula nakon urednog starta/učitavanja sistema, korisnički API servisi za kriptografske operacije, rotiranje simetričnih ključeva, upravljački interfejs koji podržava proizvoljne logičke kombinacije uslova filtera za pretragu ključnih entiteta uz eksport podataka u Excel fajlove, API interfejs za integraciju sa drugim sistemima, samostalni alati za oporavak/dekripciju podataka u offline režimu rada u slučaju da nije moguće oporaviti API servis za kriptografske operacije. - Backup 3-2-1 sistem, koji se bazira na tri nezavisne implementacije smještanja podataka, od kojih dvije moraju biti SDS storage

| | |
|---|---|
| implementacije, od čega se na dvije implementacije podaci smještaju na različitim medijumima (mehanički, ssd diskovi i sl.), od čega minimum treća implementacija mora biti fizički/prostorno izdvojena u odnosu na druge dvije i koja u predviđeno vrijeme isključivo jednostrano inicira prenos podataka. | |
| Privredni subjekat je dužan da posjeduje: minimum stručnih i kadrovskih kapaciteta koji su potrebni za izvršenje ugovora: - Minimum 1 stručno specijalizovano lice (koje će biti angažovano na realizaciji predmeta nabavke tokom cijelog ugovorenog perioda) za pružanje usluga implementacije, održavanja i tehničke podrške, koje posjeduje važeći sertifikat u rangu Linux-inženjera, sertifikat specijalizacije za SDS storage sistem, sertifikat specijalizacije za Virtuelizaciju i sertifikat specijalizacije za Visoko-dostupne klastere, kao ličnu referencu stručne i tehničke sposobnosti, pri čemu sertifikati moraju biti zasnovani po modelu izvršavanja konkretnih zadataka u realnom sistemskom okruženju (RHCE + RHCS sertifikat ili ekvivalent).<br>Navedeno se dokazuje dokazom o angažovanju radne snage i dokazom o stručnoj osposobljenosti , i to: - dokazi o angažovanju radne snage (prijava na osiguranje zaposlenog, ugovor o radu, sporazum o preuzimanju zaposlenog, ugovor o korišćenju sposobnosti drugog subjekta ili drugi akt u skladu sa zakonom), - dokaz o stručnoj osposobljenosti (sertifikat, uvjerenje ili drugi akt nadležnog organa ili organizacije). | Stručna i tehnička sposobnost |

**Kriterijumi prije izmjena**

| Opis | Očekivani odgovor ponuđača | Metod bodovanja |
|---|---|---|
| Cijena | - | - |
| • Podkriterijum kvalitet (K) vrednovaće se po osnovu parametra - iskustvo angažovanog sertifikovanog Linux-inženjera u radu sa SDS sistemom datih karakteristika, na sljedeći način:<br><br>Ponude se vrednuju po ovom parametru u odnosu na broj realizovanih projekata na istim ili sličnim poslovima iz oblasti predmeta nabavke, na osnovu podataka o kvalifikacijama i iskustvu lica (sertifikovani Linux-inženjer) | Dokaz | Relativno |

| | | |
|---|---|---|
| kojem će biti povjereno izvršenje ovog dijela predmeta nabavke.<br>Pod istim ili sličnim poslovima iz oblasti predmeta javne nabavke, podrazumjevaju se usluge implementacije, održavanja i tehničke podrške za sistem sa karakteristikama datim u nastavku:<br>primarni SDS sistem (Software-Defined-Storage) klaster implementacija sa instalisanim kapacitetom od minimum 30TB skladištenog prostora i to sve implementirano na minimum 10Gbps mrežnom okruženju; backup SDS sistem minimum istih prostornih kapaciteta kao primarni sistem; replikacija blokova podataka sa primarnog na sekundarni SDS sistem sa čuvanjem slika blokova podataka na sekundarnom sistemu minimum 7 dana.<br>Ponuđač dokazuje ovaj parametar na način što će dostaviti potvrdu/e izdatu od strane investitora, odnosno korisnika o pruženim uslugama kojom/im potvrđuje da angažovani sertifikovani Linux-inženjer kao stručni kadar ima kvalifikacije i iskustvo na istim ili sličnim poslovima iz oblasti predmeta nabavke, a koji su predviđeni tenderskom dokumentacijom. (Dostavljena potvrda treba da sadrži i opis, vrijednost predmeta nabavke, vrijeme realizacije ugovora i konstataciju da je ugovor blagovremeno i kvalitetno izvršen).<br>Napomena: Prilikom vrednovanja u obzir će se uzeti broj potvrđenih dostavljenih referenci za sva lica koja su navedena kao sertifikovani Linux inženjeri i koja će biti angažovana u realizaciji usluga koje su predmet javne nabavke.<br>Maksimalan broj bodova po ovom podkriterijumu je 10.<br>Broj bodova za ovaj podkriterijum određuje se po formuli:<br>Broj bodova (K)=(broj potvrđenih referenci)/(najveći broj potvrđenih referenci)×10 bodova.<br><br>K – broj bodova za iskustvo angažovanog sertifikovanog Linux-inženjera u radu sa SDS sistemom datih karakteristika. | | |

**Kriterijumi nakon izmjena**

| Opis | Očekivani odgovor ponuđača | Metod bodovanja |
|---|---|---|
| Cijena | - | - |

| | | |
|---|---|---|
| • Podkriterijum kvalitet (K) vrednovaće se po osnovu parametra - iskustvo angažovanog sertifikovanog Linux-inženjera u radu sa SDS sistemom datih karakteristika, na sljedeći način:<br><br>Ponude se vrednuju po ovom parametru u odnosu na broj realizovanih projekata na istim ili sličnim poslovima iz oblasti predmeta nabavke, na osnovu podataka o kvalifikacijama i iskustvu lica (sertifikovani Linux-inženjer) kojem će biti povjereno izvršenje ovog dijela predmeta nabavke.<br>Pod istim ili sličnim poslovima iz oblasti predmeta javne nabavke, podrazumjevaju se usluge implementacije, održavanja i tehničke podrške za sistem sa karakteristikama datim u nastavku:<br>primarni SDS sistem (Software-Defined-Storage) klaster implementacija sa instalisanim kapacitetom od minimum 30TB skladištenog prostora i to sve implementirano na minimum 10Gbps mrežnom okruženju; backup SDS sistem minimum istih prostornih kapaciteta kao primarni sistem; replikacija blokova podataka sa primarnog na sekundarni SDS sistem sa čuvanjem slika blokova podataka na sekundarnom sistemu minimum 7 dana.<br>Ponuđač dokazuje ovaj parametar na način što će dostaviti potvrdu/e izdatu od strane investitora, odnosno korisnika o pruženim uslugama kojom/im potvrđuje da angažovani sertifikovani Linux-inženjer kao stručni kadar ima kvalifikacije i iskustvo na istim ili sličnim poslovima iz oblasti predmeta nabavke, a koji su predviđeni tenderskom dokumentacijom. (Dostavljena potvrda treba da sadrži i opis, vrijednost predmeta nabavke, vrijeme realizacije ugovora i konstataciju da je ugovor blagovremeno i kvalitetno izvršen).<br>Napomena: Prilikom vrednovanja u obzir će se uzeti broj potvrđenih dostavljenih referenci za sva lica koja su navedena kao sertifikovani Linux inženjeri i koja će biti angažovana u realizaciji usluga koje su predmet javne nabavke.<br>Maksimalan broj bodova po ovom podkriterijumu je 10.<br>Broj bodova za ovaj podkriterijum određuje se po formuli:<br>Broj bodova (K)=(broj potvrđenih referenci)/(najveći broj potvrđenih referenci)×10 bodova.<br><br>K – broj bodova za iskustvo angažovanog sertifikovanog Linux-inženjera u radu sa SDS sistemom datih karakteristika. | Dokaz | Relativno |

**Tehnička specifikacija prije izmjena**

| Procijenjena vrijednost bez PDV | Redni broj predmeta nabavke | Opis predmeta nabavke | Bitne karakteristike predmeta nabavke | Količina | Jedinica mjere |
|---|---|---|---|---|---|
| 72000.00 | 1 | Usluga održavanja aplikacija i sistema baziranih na OpenSource tehnologijama:<br>-Usluge implementacije, tehničke podrške i održavanja aplikacija i sistema baziranih na OpenSource tehnologijama u okviru Integralnog informacionog sistema zdravstva Crne Gore | 1. OPŠTI ZAHTJEVI I INFORMACIJE<br>1.1 Generalno<br>I-1. Segmenti FZOCG sistema za koje će ponuđač pružati usluge iz predmeta javne nabavke prema traženim tehničkim i drugim zahtjevima su:<br>• Firewall/Ruter<br>• VPN koncentrator<br>• SSL gateway<br>• Virtuelizacija servera<br>• Mail sistem<br>• Sistem za mrežni monitoring<br>• Proxy sistem<br>• DNS sistem<br>• SSO sistem (Single Sign-on platforma)<br>• VPN klijent<br>• Crypto sistem<br>• SMS gateway<br>• Trustpoint sistem<br>• SDS sistem (Software-Defined-Storage)<br>I-2. Za sve navedene segmente sistema, FZOCG obezbjeđuje raspoložive hardverske resurse i resurse virtuelizovanih mašina prema datoj specifikaciji, koja čini sastavni dio tenderske dokumentacije, zatim, javne IP adrese za potrebe servisa, mrežne i druge infrastrukturne konfiguracije i parametre potrebne za instalaciju, kao i relevantne podatke potrebne za migraciju trenutnog produkcionog okruženja na ponuđena rješenja (firewall pravila, korisničke podatke, mailbox-ove, liste aktivnih profila, parametre profila i sl.) odmah po zaključenju ugovora. FZOCG za sve hardverske resurse obezbjeđuje potrebne infrastrukturne elemente i povezivanja (postavljanje opreme u rack ormaru, dovod napajanja i mrežnih kablova, optičkih veza prema storage sistemu). Zbirni resursi planiranih virtuelizovanih kapaciteta su predviđeni prema grupi virtuelnih mašina zbog fleksibilnosti preraspodjele resursa u trenutku konfiguracije virtuelnih mašina. Potrebno je da ponuđač, u odgovarajućim | 1.00 | komplet |

odgovorima za konkretne sisteme, navede pojedinačne dodjele resursa (cpu, ram, disk i sl.) virtuelnim mašinama, koje planira da iskoristi za potrebe ponuđenih rješenja, tako da zbir dodjeljenih resursa pojedinačnim konfiguracijama virtuelnih mašina ne smije prelaziti ukupan zbir planiranih kapaciteta u datoj specifikaciji.

1.2 Obavezna forma odgovora
I-3. Zahtjevi koji su postavljeni u dokumentu su naznačeni kao:
• O – Obavezan zahtjev: neophodno je da ponuđač dostavi ponudu koja ispunjava zahtjev. Neispunjenjem bilo kojeg obaveznog zahtjeva ponuda se smatra neadekvatnom i odbacuje se.
• P – Poželjan zahtjev: neophodno je da ponuđač dostavi ponudu koja je u skladu sa zahtjevom, ali on nije obavezan (eliminatoran).
• I – informacije i uputstva koje je ponuđač dužan uzeti u obzir i pridržavati ih se prilikom sačinjavanja i podnošenja ponude. Neispunjenjem bilo kojeg uputstva, datim pod ovom naznakom (I), ponuda se smatra neadekvatnom i odbacuje se.
I-4. Ponuđač je dužan da odgovore na sve zahtjeve dostavi u jednoj cjelini, tako da svaki odgovor mora da bude složen po redosljedu sadržaja navedenih tehničkih zahtjeva i da bude povezan sa rednim brojem zahtjeva u odgovoru.
I-5. Uz odgovor na svaki pojedini zahtjev, potrebno je da ponuđač jasno stavi naznaku koja predstavlja izjavu o stepenu podržanosti, koristeći sljedeće norme kvalifikacije: u potpunosti podržano (P), djelimično podržano (D). Ukoliko se ponuđač za neki od zahtjeva ne izjasni stepenom podržanosti, ponuda se smatra neadekvatnom i odbacuje se.
I-6. (P) – označava da su, u predloženim rješenjima, svi zahtjevi podržani bez poznatog tehničkog ograničenja.
I-7. (D) – označava da je zahtjev podržan uz određena tehnička odstupanja i ograničenja. Tehnička odstupanja i ograničenja moraju biti opisana i posebno objašnjena u odgovoru.
I-8. Neophodno je da ponuđač u odgovoru na svaki tehnički zahtjev, dostavi dovoljno informacija vezano za tehničke detalje

predloženih rješenja i relevantne tehničke standarde, na način da se iz odgovora može od strane FZOCG utvrditi osnovna tehnička izvodjlivost traženog zahtjeva u ponuđenom riješenju u skladu sa svim ostalim datim instrukcijama i uputstvima. Ponuda koja ne sadrži dovoljno informacija za evaluaciju smatraće se neadekvatnom i odbacuje se.
2. TEHNIČKE KARAKTERISTIKE I SPECIFIKACIJE
2.1 Opšti zahtjevi
O-1. Ponuđač je dužan navesti operativne sisteme (OS) koje koristi u ponuđenim rješenjima. Operativni sistem mora biti namjenjen za serverska okruženja i mora da podržava standardni mehanizam u cilju softverske nadogradnje i zakrpe. U slučaju naknadnog nastanka nemogućnosti nadogradnje ili zakrpe ponuđač je dužan da na zahtjev predloži drugo kompatibilno rješenje i izvrši potrebne aktivnosti implementacije tog rješenja.
O-2. Ponuđeni operativni sistem mora da podržava mehanizam za automatsku instalaciju i konfiguraciju operativnog sistema bez interakcije administratora u toku instalacionog procesa. Potrebno je navesti preduslove koje FZOCG treba da obezbijedi za slučaj korišćenja ovog mehanizma.
I-9. Ponuđač je dužan ponuditi implementaciju, održavanje i tehničku podršku za sva ponuđena rješenja. Usluge implementacije, između ostalog, obuhvataju i eventualnu privremenu instalaciju i konfiguraciju ponuđenih rješenja u cilju preuzimanje postojećeg produkcionog okruženja na održavanje, zatim, migraciju podataka i integraciju sa ostalim IT okruženjem.
I-10. Ponuđač je dužan ponuditi arhitekturu rješenja, koja se zasniva na OpenSource tehnologijma, na način da ne postoje nikakva ograničenja po pitanju uslova licenciranja po parametrima okruženja (kao npr. po broju istovremenih konekcija, broju korisnika, broju procesora, broju lokacija i sl.) i u slučaju prekida saradnje sva prava korišćenja za sve sisteme moraju ostati u vlasništvu FZOCG za neograničenu internu upotrebu u okviru Integralnog informacionog sistema zdravstva.
I-11. Sva ponuđena riješenja, u okviru redudantnih/klaster cjelina pojedinačnih

sistemskih segmenata, moraju biti jednobrazna po pitanju izbora tehnologija, odnosno nije dozvoljeno korišćenje jedne tehnologije na jednom klaster nodu, dok na drugom nodu u istom klasteru da se koristi druga tehnologiju za realizaciju istog servisa za koji je predviđen taj klaster. Takođe, u konačnoj implementaciji, sve verzije softvera i konkretne softverske komponente moraju biti iste na svim klaster nodovima, na način da se nodovi razlikuju samo u podešavanjima.
I-12. Ponuđač ne smije unazaditi sistem po pitanju softverskih verzija, odnosno koristiti verzije softvera starije od onih koje standardno dolaze uz instalaciju operativnog sistema ili od onih verzija koje su dostupne kroz standardni kanal softverske nadogradnje (onaj kanal koji je podešen odmah nakon standardne instalacije OS-a), što ne ograničava ponuđača da koristi još novije verzije, pod uslovom da se radi o stabilnim verzijama i da ih sam pripremi za instalaciju, ili da koristi zadnju verziju, ili da pripremi izmjenjenu verziju (patch) konkretne softverske komponente.
I-13. Ponuđač može da, u cilju zadovoljenja određenih tehničkih zahtjeva, dodatno izvrši prilagođavanja na sistemu, izvrši instalaciju dodatnih softverskih komponenti, ili da izvrši nadogradnju/izmjenu softverskih komponenti (patch i sl.), razvije pomoćne programe (backup rutine i sl.), razvije softverske module u okviru postojećih softverskih komponenti ili razvije administratorske/korisničke interfejse (web i sl.), ili da razvije određenu funkcionalnost u cjelosti.
I-14. Ponuđač je dužan da kompletnu implementaciju svih ponuđenih rješenja, kao i tražena proširenja postojećih produkcionih sistema, izvrši u roku koji je dat u tenderskoj dokumentaciji. FZOCG obezbijeđuje ispunjenost preduslova potrebnih za izvršenje aktivnosti u datom vremenskom roku, što uključuje: neometan pristup server sali i raspoloživost hardverskih, podataka i drugih resursa na lokaciji naručioca, opisanih u tenderskoj dokumentaciji.
I-15. Obzirom da je većina sistema u produkcionoj upotrebi gdje se toleriše veoma mali downtime ne duži od 10 min, neophodno je da ponuđač prilikom

implementacije ponuđenih rješenja koristi prvo pasivni nod (backup nod) u okviru klaster grupa, a zatim da prebaci produkcioni sistem na pasivni nod, kako bi nastavio sa implementacijom na preostalim nodovima. Kod grupa koje imaju active/active nodove, potrebno je prvo proširiti sistem sa novim nodovima (koristiti predviđene pomoćne virtuelizovane i hardverske resurse, date specifikacijom iz tenderske dokumentacije), pa tek onda migrirati produkcioni sistem na tako novoimplementirane nodove kako bi se konačno oslobodili preostali nodovi za nastavak implementacije ponuđenih riješenja. Kod grupa koje imaju više od dva noda u klasteru, moguće je privremeno isključivanje do dva noda (na primjer odgovarajući par), kako bi se oslobodili postojeći produkcioni hardverski ili virtuelizovani resursi za novu implementaciju, a sve pod uslovom da u klaster grupi uvijek ostanu barem dva noda u produkciji. Za implementaciju pojedinačnih nodova, koji nisu sastavni dio klastera ili cijelina, ponuđač može privremeno koristiti predviđene pomoćne hardverske i virtuelizovane resurse, date specifikacijom iz tenderske dokumentacije, do završetka implementacije. Sve aktivnosti je potrebno izvršiti uživo na sistemu.
2.2 Posebni zahtjevi i instrukcije za implementaciju ponuđenih rješenja
I-16. Ponuđena rješenja moraju da zadovoljavaju sve industrijske standarde predviđene tehničkim zahtjevima, kako bi integracija sa postojećim produkcionim okruženjem bila izvodljiva.
I-17. Platforma za virtuelizaciju se sastoji od KVM hipervizora, koji su redudantno povezeni na zajednički SDS storage sistem (10Gbps mreža), a međusobno i prema ostatku sistema su povezani preko redudantnih veza na mrežne switcheve. Moguće je isključiti do dva hipervizora istovremeno iz produkcionog klastera i to u strogo predviđenom vremenskom rasponu, a sve u cilju implementacije ponuđenog rješenja u ovom segmentu. Prije početka implementacije, sve virtuelne mašine sa hipervizora koji se privremeno isključuju će biti migrirane na preostale hipervizore a nakon implementacije ponuđenog rješenja,

migrirane virtuelne mašine će biti vraćene na iste te hipervizore.
I-18. Za implementaciju ponuđenog rješenja u SSL gateway segmentu, FZOCG obezbijeđuje sve podatke potrebne za migraciju na ponuđeno rješenje (username, pin/tan liste, nazive institucija i korisnika, grupa privilegija, kao i međusobne relacije entiteta, x509 sertifikate).
I-19. Platforma VPN koncentratora se sastoji od dva virtuelizovana servera koja povezuju udaljene lokacije, koje se sastoje od jednog ili više računara (lica, ustanove, punktovi itd.). Određene lokacije preko zajedničkog Internet linka ostvaraju više paralelnih VPN konekcija
O-3. Ponuđač je dužan implementirati platformu za virtuelizaciju, uz zadovoljenje svih traženih tehničkih zahtjeva, u koracima od po dva noda u paru, na način da sve aktivnosti prvog nivoa podrške budu izvodljive preko svih serverskih nodova odmah nakon završetka sveukupne implementacije.
O-4. Vremenski raspon implementacije ponuđenog rješenja, u segmentu platforme za virtuelizaciju, za jedan par nodova ne može biti duži od 4h. Potrebno je izvršiti live backup (snapshot) svih virtuelnih mašina na svim hipervizorima, nakon završetka implementacije ponuđenog rješenja.
O-5. Ponuđač je dužan implementirati plaformu VPN koncentratora tako da je moguće konkurentno funkcionisanje većeg broja TCP konekcija sa računara udaljene lokacije koji su preko više paralelnih VPN konekcija povezani na sistem (preko zajedničkog Internet linka na udaljenoj lokaciji
2.3 Tehnička podrška
I-20. FZOCG obezbjeđuje prvi nivo podrške koji podrazumijeva svakodnevne operativne aktivnosti na sistemima koji su predmet javne nabavke. Ponuđač obezbjeđuje drugi nivo tehničke podrške za sve komponente implementiranih sistema.
O-6. Ponuđač je dužan da ponudi drugi nivo tehničke podrške koji podrazumijeva operativne aktivnosti instalacije, konfiguracije, migracije, konsaltinga, preventivnog održavanja, otklanjanje tehničkih problema i izvršenje preporučenih upgrade-a komponenti sistema, kao i

definisanje operativnih procedura za kvalitetno sprovođenje prvog nivoa podrške (na dnevnom, nedjeljnom i mjesečnom nivou).
P-1. Poželjno je da ponuđač u toku trajanja ugovora, a na zahtjev FZOCG, blagovremeno obezbijedi procedure i dokumentaciju koja sadrži procedure, detaljne opise, instalaciju, administraciju i korisničke priručnike za sve djelove sistema.
P-2. Ponuđači se pozivaju da dostave opise dodatnih funkcionalnosti sistema koje nijesu zahtijevane, a koje mogu služiti unapređenju sistema.
O-7. Neophodno je da ponuđač definiše procedure za prijavu problema kao i vremena odziva za sljedeće nivoe problema:
• Urgentni nivo problema
• Visok nivo problema
• Srednji nivo problema
• Nizak nivo problema.
I-21. Definicije nivoa problema su sledeće:
Urgentni nivo problema Sistem nije funkcionalan.
Visok nivo problema Problemi u dostupnosti servisa, ali većina korisnka može da dobije servis.
Srednji nivo problema Problemi koji trenutno ne ugrožavaju funkcionalnost servisa, ali mogu da utiču na funkcionalnost ukoliko se ne pristupi blagovremenom rješavanju
Nizak nivo problema Manji problemi ili tehnički zahtjevi koji ne utiču na funkcionalnost sistema

O-8. Za sve tipove problema ponuđač mora obezbjeđivati vrijeme privremenog i trajnog rješenja od momenta prijave problema, kao i raspoloživost resursa tehničke podrške za slučaj problema po principu 24/7/365.
Maksimalne vrijednosti vremena privremenog odnosno trajnog rješenja problema u odnosu na nivo problema su date u tabeli:
Nivo problema Vrijeme privremenog rješenja Vrijeme trajnog rješenja
Urgentni 8h 36h
Visok 24h 1 nedjelja
Srednji 1 nedjelja 4 nedjelje
Nizak 3 nedjelje 6 nedjelja

O-9. Ponuđač je u obavezi da obezbjedi mogućnost prijave problema 24 sata dnevno

i to na sljedeće načine: WEB portal za prijavu problema; e-mail; fax i telefon. U ponudi je neophodno navesti informacije za sve tražene načine prijave problema.
2.4 Sistemi i platforme
2.4.1 Firewall/Ruter
O-10. Firewall/ruter rješenje mora da podržava standardni set funkcionalnosti:
• Stateful i Stateless opciju filteringa paketa.
• 802.1q (vlan tagging)
• Troubleshooting alati (ping, traceroute, log)
• NAT (Network Address Translation)
• PAT (Port Address Translation)
• DHCP server (server za dodjelu dinamičkih IP adresa)
• Statičko rutiranje
• Backup/Restore konfiguracija,
• Kontrola udaljenog administratorskog pristupa, na način da pojedinačni privilegovani administratori, zaduženi za podešavanja Firewall/Ruter sistema, mogu pristupiti samo sa unaprijed određenih IP adresa.
O-11. Firewall/ruter rješenje mora da podržava napredni set funkcionalnosti:
• Združivanje mrežnih interfejsa (active/passive, agregacija)
• Rutiranje na osnovu polisa (tip saobraćaja, source i destination IP adrese, portovi)
• QoS (shaping i prioritetizacija na osnovu polisa ili odgovarajućih bitova u IP hederu paketa)
• OSPF dinamički ruting protokol, na način da omogućava sinhronizaciju jedne ili više ruting tabela operativnog Sistema
• Adaptivna performansna podešavanja za mrežnu brzinu/kašnjenje
• Adaptivni menadžment procesa i memorije u cilju efikasnog izvršavanja procesa u multiprocesorskom okruženju sa više sistemskih magistrala
• Automatsko balansiranje procesorskih prekida između jezgara u realnom vremenu u skladu sa uslovima rada sistema.
• Aplikativni balanser saobraćaja po HTTP protokolu: prema različitim unutrašnjim putanjama i uz ravnomjernu distribuciju saobraćaja; zadržavanje saobraćaja sesije prema istoj unutrašnjoj putanji do završetka sesije; praćenje ispravnosti unutrašnjih putanja i preusmjeravanje saobraćaja prema ispravnim putanjama u slučaju ispada.
O-12. Firewall/ruter rješenje mora da

podržava visoko-dostupne (High Availiability - HA) konfiguracije (active/passive).
O-13. Firewall/ruter rješenje treba da omogućava administratorski interfejs/alat, ili konfiguracione fajlove, na način da podržava izvršenje tipičnih dnevnih aktivnost prvog nivoa podrške.
I-22. Tipični poslovi obavljanja prvog nivoa podrške kod ovog sistema podrazumijeva definisanje i mijenjanje sljedećih parametara: interfejsa, firewall pravila, mrežnih ruta, NAT; zatim, backup/restore aktivnosti i analizu logova.
I-23. Firewall sistem je u produkcionom okruženju implementiran u modu active/backup na dva servera prema specifikaciji hardverskih resursa iz tenderske dokumentacije.
2.4.2 VPN Koncentrator
O-14. VPN koncentrator rješenje mora da podržava opciju za terminaciju IPSEC tunela.
O-15. VPN koncentrator rješenje mora da podržava AES, SHA i Diffie Hellman Grupe podešavanja za IKE i ESP enkripcione transformacije, minimum: aes128, aes192, aes256, sha1,sha256,sha384,dh-2,5,14,15.
O-16. VPN koncentrator rješenje mora da podržava pojedinačno ili kombinaciju opcija, PSK, x509, i password identifikaciju udaljenih lokacija, koje su ukačene po IPSEC protokolu. Podržane kombinacije navedenih opcija, ili podešavanje pojedinačnih opcija, moraju da podržavaju kačenje sledećih klijenata: Cisco VPN klijent, Linux klijenti, Apple iPhone klijent, Windows 7 i Windows 10 klijent, Juniper klijent.
O-17. VPN koncentrator rješenje mora da podržava opciju za NAT-T (nat traversal) protokol.
O-18. VPN koncentrator rješenje mora da podržava opciju za DPD (dead peer detection) protokol.
O-19. VPN koncentrator rješenje mora da podržava opciju za IP kompresiju tuneliranih paketa.
O-20. VPN koncentrator rješenje mora da podržava dinamički protokol za razmjenu ključeva IKEv1 i IKEv2.
O-21. VPN koncentrator rješenje mora da podržava automatsko spuštanje mrežnih ruta po IKEv1 i IKEv2 protokolu, za svaku klijentsku VPN konekciju pojedinačno.

O-22. VPN koncentrator rješenje mora da podržava uspostavljanje PPTP tunela prema udaljenim lokacijama (MSCHAPv2, MPPE). Samo se jedan server u klaster grupi koristi za ovu namjenu, na način što se unaprijed odredi od strane FZOCG.
O-23. VPN koncentrator rješenje mora da podržava PKI (Public Key Infrastructure) elemente koji su potrebni za ažuriranje x.509 sertifikata – (CA, generate, revoke, crl liste, crl URL, OCSP provjeru).
O-24. VPN koncentrator mora da podržava konfiguraciju access lista po IPSEC konekciji.
O-25. VPN koncentrator rješenje mora da podržava osnovni i napredni set firewall/ruter funkcionalnosti iz tehničkih zahtjeva.
O-26. VPN koncentrator rješenje mora da podržava rad u u grupi od više koncentratora, na način da u slučaju ispada jednog koncentratora, sve raskinute udaljene konekcije mogu da se preraspodjele na preostale koncentratore u grupi, odnosno svi koncentratori unutar grupe moraju da imaju ulogu aktivnih nodova prema kojima se automatski uspostavljaju VPN konekcije udaljenih lokacija.
O-27. VPN koncentrator riješenje mora da pruža NTP servis ostatku mreže FZOCG, na način da se sinhronizuje sa barem 4 udaljena NTP referentna izvora, kao i da su svi koncentratori referentno sinhronizovani između sebe.
O-28. VPN koncentrator rješenje treba da omogućava administratorski interfejs/alat, ili konfiguracione fajlove, na način da podržava izvršenje tipičnih dnevnih aktivnost prvog nivoa podrške.
I-24. Tipični poslovi obavljanja prvog nivoa podrške kod ovog sistema podrazumijeva definisanje i mijenjanje sljedećih parametara: korisnika, x509 sertifikata, interfejsa, firewall pravila, ruta, NAT; zatim, backup/restore aktivnosti i analizu logova.
I-25. VPN koncentrator sistem je u trenutnom produkcionom okruženju implementiran u modu active/active (svi serveri imaju ulogu aktivnih nodova), na dvije virtuelizovane mašine prema specifikaciji virtuelizovanih resursa iz tenderske dokumentacije.
2.4.3 SSL gateway

O-29. SSL gateway rješenje mora da podržava terminaciju SSL/TLS zaštićenih konekcija preko HTTP protokola (HTTPS tip konekcije) za udaljene lokacije (IP adresa udaljenih lokacija nisu unaprijed poznate).
O-30. SSL gateway rješenje mora da podržava konfiguraciju zasebnog x509 sertifikata za svaki domen/profil HTTPS konekcije pojedinačno.
O-31. SSL gateway rješenje mora da podržava identifikaciju HTTPS konekcija po modelu korisničkog naloga i pin koda.
O-32. SSL gateway rješenje treba da podržava naprednu identifikaciju HTTPS konekcija, za sveukupan saobraćaj po tim konekcijama, po modelu PIN/TAN sistema (bankarski standard za authentifikaciju baziran na jednokratnim kodovima za autentifikaciju).
O-33. SSL gateway rješenje mora da podržava konfiguraciju unutrašnje URL putanje na koju se preusmjeravaju dolazni zahtjevi, za svaki profil spoljašnje HTTPS konekcije pojedinačno, na način da omogućava privilegije pristupa prema unutrašnjim URL putanjama po grupama identifikovanih korisnika (privilegije na nivou grupa).
O-34. SSL gateway mora da omogućava WEB administratorski i korisnički interfejs, na način da se prikaz interfejsa automatski prilagođava veličini ekrana na uređaju sa kojeg se pokreće interfejs (mobile-responsive karakteristika).
O-35. SSL gateway rješenje treba da omogućava administratorski interfejs na način da podržava izvršenje tipičnih dnevnih aktivnost prvog nivoa podrške.
O-36. SSL gateway rješenje treba da omogućava korisnički interfejs na način da podržava korisnički pristup unutrašnjim URL putanjama na osnovu date grupe privilegija i to nakon uspješne autentifikacije sa korisničkim nalogom, pinom i jednokratnom lozinkom sa TAN lista, zatim, da omogućava interfejs za promjenu PIN-a, generisanje novih TAN lista, kao i vizuelni indikator da je lista sa TAN kodovoima pri kraju (uskoro istrošena).
O-37. SSL gateway mora da podržava visoko-dostupne (High Availiability - HA) i skalabilne konfiguracije, na način da ravnomjerno distribuira zahtjeva prema

aplikativnim instancama. U slučaju ispada nekog od nodova toleriše se ponovno uspostavljanje konekcija i identifikacija korisnika.
I-26. Tipični poslovi obavljanja prvog nivoa podrške kod ovog sistema podrazumijeva definisanje i ažuriranje sljedećih parametara: ustanova, korisnika, grupa privilegija, PIN/TAN lista, unutrašnjih URL putanja).
I-27. FZOCG obezbijeđuje važeći potpisani x 509 sertifikat, do 5 domena, koji se sastoji od javnog i privatnog ključa, kao i javnog ključa CA koja je izdala sertifikat, a sve u standardnom elektronskom formatu.
I-28. Za implementaciju SSL gateway rješenja,u skladu sa datim tehničkim zahtjevima, su previđene virtuelizovane mašine prema specifikaciji virtuelizovanih resursa iz tenderske dokumentacije.
2.4.4 Virtuelizacija servera
O-38. Platforma za virtuelizaciju servera mora da podržava virtuelizaciju gost mašina (virtuelne mašine), baziranu na KVM tehnologiji, i to bez izmjena na nivou gost mašine, uz podržane hipervizor servere x86_64 procesorske arhitekture (cpu namjene za virtuelizaciju).
O-39. Platforma za virtuelizaciju servera mora da podržava Linux OS (32bit i 64bit) gost virtuelne mašine.
O-40. Platforma za virtuelizaciju servera mora da podržava sledeće Microsoft Windows  gost virtuelne mašine: Windows Server 2012, Windows 2003 server, Windows 2008 server, Windows XP, Windows 7. Platforma za virtuelizaciju mora da podržava rješenje za migraciju (OS i podaci) fizički odvojenih računara (sa CD/DVD uređajemi mrežnom karticom) u gost virtuelne mašine (sa kompatibilnom konfiguracijom – broj procesora, količina radne memorije, veličina diska, magistrale, grafička kartica itd.) za sledeće Microsoft Windows operativne sisteme: Windows XP, Windows 7 i Windows 2003 server.
O-41. Platforma za virtuelizaciju servera mora da podržava kreiranje novih virtuelnih mašina po unaprijed definisanom template-u (broj procesora i diskova, veličina diska i ram memorije, preinstalirani operativni sistem).
O-42. Platforma za virtuelizaciju servera mora da podržava tehniku pozajmljivanja

memorija između virtuelnih mašina (memory-ballooning) u slučaju kompatibilnog OS-a na gost virtuelnoj mašini.
O-43. Platforma za virtuelizaciju servera mora da podržava kreiranje backupa od diska virtuelne mašina bez obaranje same virtuelne mašine (shutdown), odnosno neosjetno za rad virtuelne mašine (live-snapshot funkcionalnost).
O-44. Platforma za virtuelizaciju servera mora da podržava NAS/NFS, Fiber channel i iSCSI topologije veza prema storage sistemu, kao i da podržava integraciju preko interfejsa za smještanje blokova podataka (block disk) na SDS sistem na kojem će se nalaziti glavni raspoloživi kapaciteti sa skladištenje podataka.
O-45. Platforma za virtuelizaciju mora da podržava klasterizovani fajl sistem OCFSv2.
O-46. Platforma za virtuelizaciju mora da podržava podešavanje I/O virtuelizacije mrežnih interfejsa i direktnu dodjelu virtuelizovanog mrežnog segmenta mašinama tako da je moguća live migracija između odgovarajućeg para hipervizora.
O-47. Platforma za virtuelizaciju servera treba da omogućava administratorski interfejs/alat, ili konfiguracione fajlove, na način da podržava izvršenje tipičnih dnevnih aktivnost prvog nivoa podrške.
I-29. Tipični poslovi obavljanja prvog nivoa podrške kod ovog sistema podrazumijeva kreiranje virtuelnih mašina i njihovo podešavanje, migracija virtuelnih mašina između hipervizora “uživo” (live migration), kreiranje i dodjela mrežnih interfejsa, “uživo” backup virtuelnih mašina (live snapshot), migracija Win7/XP/2003server fizičkih mašina u gost virtuelne mašine, automatizovana migracija svih virtuelnih mašina sa jednog hipervizora na drugi.
I-30. Platforma za virtuelizaciju se u produkcionom okruženju sastoji od šest hipervizora (prema specifikaciji hardverskih resursa iz tenderske dokumentacije), povezana na zajednički SDS storage sistem, redudantnim 10Gbps, koja omogućavaju uživo migraciju mašina između hipervizora, uživo backup (snapshot) diska virtuelnih mašina, kao i konverziju između storage image formata prema potrebi. Za namjenu podrške migraciji fizičkih Windows računara u gost virtuelne mašine je predviđen

odvojeni server (prema specifikaciji hardverskih resursa iz tenderske dokumentacije).
2.4.5 Mail sistem
O-48. Mail sistem rješenje treba da podržava standardne protokole mail komunikacije uz obaveznu enkripciju preko istih ili odvojenih portova: POP3, SMTP, IMAP.
O-49. Mail sistem rješenje treba da podržava SUBMISSION port za slanje mailova, na način da je obavezna prethodna autentifikacija korisnika prije slanja/transfera maila prema serveru. Slanje mailova preko standardnog SMTP porta, od strane korisnika FZOCG, nije dozvoljeno, već se standardni SMTP port koristi samo za primanje mailova za lokalne domene.
O-50. Mail sistem rješenje mora da podržava SPF i DKIM mehanizme prema DMARC preporuci, kao i da obezbjeđuje ARC implementaciju. Mail sistem rješenje mora da podržava PFS mehanizam.
O-51. Mail sistem rješenje treba da podržava Webmail interfejs. Webmail interfejs mora da podržava opcije za auto-responder, email filtere i personalizovane potpise, pregled i konstruisanje HTML email poruka.
O-52. Mail server rješenje mora da podržava deduplikaciju i kompresiju mejl sadržaja na način da se minimizuje skladišteni prostor tako da isti mejl sadržaj poslat/primljen na više adresa bude uskladišten tačno jednom. Mail server rješenje mora da podržava brzu pretragu (ispod 1s) za mejl sanduče koje broji velike količine mejlova (50.000 mejlova i više).
O-53. Mail server rješenje treba da podržava Anti-Spam i Anti-Virus mehanizme zaštite po korisničkom nalogu za dolazni i odlazni saobraćaj. Mail server rješenje mora da podržava definisanje proizvoljne anti-spam politike određivanja da li je mejl sadržaj spam.
O-54. Mail server rješenje treba da podržava konfigurisanje (uključivanje/isključivanje) pojedinačnih servisa po korisničkom nalogu i to za sledeće pojedinačne privilegije/pristupe: SMTP, POP3, IMAP, Anti-Spam i Anti-Virus, podešavanje filtera i preusmjeravanje maila.
O-55. Mail server rješenje mora da podržava

korisničke klase servisa za ograničenja i propusne kontrole u jedinici vremena (minuti) za odlazni saobraćaj u predefinisanim periodima i danima u toku nedjelje, a sve mjereno pojedinačno po korisničkom nalogu/adresi, uz mogućnost definisanja proizvoljnih smtp-greška poruka: maksimalni broj mejlova u jedinici vremena, maksimalni broj primalaca u jedinici vremena, maksimalnu ukupnu veličinu mejlova u jedinici vremena, maksimalnu veličinu pojedinačnog mejla.
O-56. Mail server rješenje mora da podržava prijemne klase servisa za ograničenja i propusne kontrole u jedinici vremena (minuti) za dolazni saobraćaj u predefinisanim periodima i danima u toku nedjelje, uz mogućnost definisanja proizvoljnih smtp-greška poruka: maksimalni broj konekcija u jedinici vremena, maksimalni broj pokušaja isporuke u jedinici vremena na osnovu broja aktivnih RBL listinga (predefinisane liste), maksimalni broj pokušaja isporuke na osnovu regexp pretrage po hostname/helo parametrima SMTP konekcije.
O-57. Mail server rješenje mora da podržava blokiranje isporuke mejla na osnovu otiska SSL sertifikata udaljenog servera koji pokušava isporučiti poštu.
O-58. Mail server rješenje mora da podržava definisanje proizvoljnog perioda i privremene smtp-greške koju će sistem javljati za zakazana održavanja sistema, u okviru kojeg privremeno neće biti dozvoljeno primanje ili slanje mejlova.
O-59. Mail server rješenje mora da podržava automatsko serversko dodavanje sadržaja na kraju odlaznog mejla (prema destinacijama van sistema). Sadržaj se definiše u HTML i TXT formatu po korisniku, a odgovarajuća varijanta se dodaje u zavisnosti od tipa mejla (HTML i/ili TXT).
O-60. Mail server rješenje mora da obezbjeđuje konfiguraciju u skladu sa vodećim preporukama, tako da zadovoljava sve testove i propratne preporuke na online Internet testu MXToolBox. Online adresa preko koje se testira je: https://mxtoolbox.com.
O-61. Mail sistem rješenje treba da omogućava administratorski interfejs/alat, ili konfiguracione fajlove, na način da

podržava izvršenje tipičnih dnevnih aktivnost prvog nivoa podrške.
I-31. Tipični poslovi obavljanja prvog nivoa podrške kod ovog sistema podrazumijeva kreiranje, brisanje korisničkih naloga, upravljanje mejl aliasima, promjena lozinke, backup mailova po korisničkom nalogu, kao i analiza logova.
I-32. Za implementaciju mail sistema je predviđena jedna virtuelna mašina, prema specifikaciji virtuelizovanih resursa iz tenderske dokumentacije.

2.4.6 Sistem za mrežni monitoring
O-62. Sistem za mrežni monitoring mora da podržava praćenje dostupnosti servisa po TCP, UDP i ICMP (ping) mrežnim protokolima.
O-63. Sistem za mrežni monitoring mora da podržava mehanizme za praćenje dostupnosti servisa (na primjer: http, mail i sl.).
O-64. Sistem za mrežni monitoring mora da podržava mehanizme za prikupljanje informacija po SNMP protokolu, koristeći mehanizam “SNMP trap” i prikupljanje SYSLOG logova, te generisanje događaja na osnovu prikupljenih informacija. Obavezna je implementacija slanja SNMP trap poruka u slučaju ispada agregacija mrežnih interfejsa na serverskim nodovima koji imaju podešenu mrežnu redudantnost.
O-65. Sistem za mrežni monitoring mora da podržava ručno ubacivanje nodova za praćenje, kao i automatsko traženje dostupnih nodova na osnovu zadate mreže, i automatsko traženje dostupnih servisa na pronađenom nodu.
O-66. Sistem za mrežni monitoring mora da podržava slanje email poruka u sastavnom dijelu notifikacionih mehanizama.
O-67. Sistem za mrežni monitoring mora da podržava generisanje i prikazivanje grafika praćenih podataka (na primjer: in/out bytes i sl.).
O-68. Sistem za mrežni monitoring treba da omogućava administratorski interfejs/alat, ili konfiguracione fajlove,  na način da podržava izvršenje tipičnih dnevnih aktivnost prvog nivoa podrške.
I-33. Tipični poslovi obavljanja prvog nivoa podrške kod ovog sistema podrazumijeva administraciju pravila za praćenje, pregled

podataka i relevantnih izvještaja stanja.
I-34. FZOCG će samostalno izvršiti unos pravila za praćenje u sistemu za mrežni monitoring, nakon sveobuhvatne implementacije svih ostalih sistema.
I-35. Za implementaciju sistema za mrežni monitoring je predviđena jedna virtuelna mašina, prema specifikaciji virtuelizovanih resursa iz tenderske dokumentacije.
2.4.7 Proxy sistem
O-69. Proxy sistem mora da podržava keširanje web saobraćaja (HTTP).
O-70. Proxy sistem mora da podržava filtriranje web zahtjeva po tipu sadržaja (exe, zip, doc, excel i slične formate).
O-71. Proxy sistem mora da podržava filtriranje web saobraćaja po ključnim riječima.
O-72. Proxy sistem mora da podržava filtriranje web zahtjeva po URL adresama.
O-73. Proxy sistem mora da podržava konfiguraciju prava pristupa po jednoj ili više korisničkih IP adresa, po danima u nedjelji.
O-74. Proxy sistem mora da podržava mehanizme za integraciju sa trećim sistemima za analizu/adaptaciju sadržaja (na primjer: u cilju antivirus skeniranje, ubacivanje upozorenja o sumnjivom sadržaju i sl. ).
O-75. Proxy sistem mora da podržava transparentno presretanje i filtriranje enkriptovanog web saobraćaja (https).
O-76. Proxy sistem mora da omogućava administratorski interfejs/alat, ili konfiguracione fajlove, na način da podržava izvršenje tipičnih dnevnih aktivnost prvog nivoa podrške.
I-36. Tipične dnevne aktivnosti na ovom sistemu podrazumijevaju konfiguraciju različitih podržanih filtera i polisa.
I-37. Za implementaciju Proxy sistema je prdviđena jedna virtuelna mašina, prema specifikaciji virtuelizovanih resursa iz tenderske dokumentacije.
2.4.8 DNS sistem
O-77. DNS sistem mora da podržava konfiguracije autoritativnog, slave, forvardera ili kešing dns sistema.
O-78. DNS sistem mora da minimalno podržava sledeće resurs rekorda u okviru konfiguracije zona:
• A (address record)
• NS (name server record)

• PTR (pointer record)
• CNAME (canonical name record)
• TXT (text record)
• SPF (sender policy framework record)
• MX (mail exchange record)
• SRV (service locator).
O-79. DNS sistem mora da podržava AXFR mehanizam za transfer zona.
O-80. DNS sistem mora da podržava Split-Horizon funkcionalnost.
O-81. DNS sistem treba da omogućava administratorski interfejs/alat, ili konfiguracione fajlove, na način da podržava izvršenje tipičnih dnevnih aktivnost prvog nivoa podrške.
I-38. Tipične dnevne aktivnosti na ovom sistemu podrazumijevaju konfiguraciju različitih tipova resurs rekorda.
I-39. Za implementaciju DNS sistema u produkcionom okruženju je predviđena jedna virtuelna mašina prema specifikaciji virtuelizovanih resursa iz tenderske dokumentacije, kao i jedna udaljena serverska instanca na Internetu za slave implementaciju.
2.4.9 SSO sistem
I-40. Zbog većeg broja servera kojima administratori FZOCG pristupaju svakodnevno, zatim, unapređenja kontrole pristupa i sigurnosti svekupnog sistema, kao i potrebe jednostavnog prenosa fajlova između servera odvojenih mrežnih segmenata, potrebno je implemenitrati SSO sistem sa zaštićenim mrežnim direktorijumom.
O-82. Ponuđač mora da implementira riješenje za SSO sistem, koje omogućava administratorski pristup serverima sa radnih stanica, po modelu identifikacije preko korisničkog naloga/passworda unošenjem passworda samo jednom (SSO / single-sign-on), nakon čega se administratoru odobrava pristup (preko SSH ili drugog mehanizma) bez ponovne autentifikacije passwordom, i sve to direktno sa radne stanice administratora.
O-83. SSO sistem mora da omogući administratoru način da se odjavi, sa čime mu se uklanjaju prethodno date privilegije pristupa bez ponovnog unošenja passworda.

O-84. Mogućnost pristupa serverima na standardan način preko

username/passworda mora ostati nepromjenjena, za slučaj da administrator ne želi da koristi u datom momentu SSO sistem.
O-85. Kada administrator pristupi serveru, potrebno je da mu se automatski poveže personalizovani mrežni direktorijum na tom serveru sa centralne lokacije, za koji samo on ima prava pristupa (drugi ulogovani administratori ne mogu da pristupe tom direktorijumu za slučaj da se nalaze na istom serveru). Ukoliko se administrator uloguje na više servera istovremeno, mrežni direktorijum mora biti dostupan na svim serverima, zadržavajući prava pristupa samo tom adminstratoru.
O-86. Transfer fajlova između servera kojem se pristupa i mrežnog direktorijuma mora biti enkriptovan sa odgovarajućim algoritmom, koji mora biti industrijski standard. Navesti algoritam koji će se koristiti za enkripciju u ponuđenom riješenju.
I-41. Za implementaciju svih navedenih tehničkih zahtjeva SSO sistema su predviđene virtuelne mašine, prema specifikaciji virtuelizovanih resursa iz tenderske dokumentacije.
2.4.10 VPN klijent
O-87. Ponuđač mora da obezbijedi VPN klijent rješenje, koje je podržano na Linux distribucijama koje se trenutno koriste u FZOCG (zadnja verzija Ubuntu LTS, CentOS i RockyLinux distribucije), tako da podržava automatsko uspostavljanje IPSec konekcija (podržana oba protokola IKEv1 i IKEv2) prema VPN koncentratorima FZOCG, sa podržanim automatskim prihvatanjem mrežnih ruta od strane VPN koncentratora, kao i provjeru validnosti serverskog sertifikata po CRL i/ili OCSP putanji koja je upisana u sertifikatu.
O-88. VPN klijent rješenje treba da omogućava administratorski interfejs/alat, ili konfiguracione fajlove, na način da podržava izvršenje tipičnih dnevnih aktivnost prvog nivoa podrške.
O-89. Potrebno je da ponuđač obezbijedi odgovarajuću podršku za dijagnostiku prilikom problema u uspostavljanju IPSEC konekcija sa Linux i Microsoft Windows operativnih sistema, kao i sa drugih podržanih uređaja.
I-42. Tipične dnevne aktivnosti na VPN

klijentskom sistemu podrazumijevaju: konfiguraciju IPSEC klijentskih tunela.
I-43. VPN klijentsko riješenje se u produkcionom okruženju instalira od strane administratora FZOCG prema procedurama koje definiše ponuđač, odnosno nije obaveza ponuđača da izvršava konkretnu instalaciju VPN klijenta, već samo da obezbijedi VPN klijentsko riješenje prema tehničkom zahtjevu.
2.4.11 SMS gateway
O-90. SMS Gateway mora da podržava integraciju sa SMS centrom mobilnih operatora po protokolu SMPP verzija 3.3 i 3.4.
O-91. SMS Gateway mora da podržava udruživanje više paralelnih konekcija prema istom SMS centru mobilnog operatora i ravnomjerno balansiranje slanja SMS poruka preko tako udruženih konekcija.
O-92. SMS Gateway mora da podržava podešavanje različitih profila konekcija prema SMS centrima mobilnih operatora sa mogućnošću podešavanje parametara SMPP protokola (profili za različite mobilne operatore sa različitim varijantama SMPP podešavanja).
O-93. SMS Gateway mora da podržava integraciju korisničkih servisa preko REST web servisa: za slanje poruka, primanje poruka preko kratkog koda, kao i za dobijanje povratnih notifikacija o uspješnosti isporuke.
O-94. SMS Gateway mora da podržava mehanizam autentifikacije REST web servisa preko dodijeljenog sigurnosnog tokena (token se prenosi kao “query” parametar u HTTP zahtjevu web servisa).
O-95. SMS Gateway mora da podržava podešavanje više korisničkih profila u okviru kojih se definišu parametri servisa: sigurnosni token za REST web servis, dozvoljeni filteri telefonskih brojeva, dozvoljeni SMS centri za upotrebu, maksimalno vrijeme života poruke (ttl), predefinisani templejt REST adrese za slanje povratnih notifikacija.
O-96. SMS Gateway mora da podržava podešavanje REST templejta adrese koja će se prozivati za svaku dobijenu notifikaciju o uspješnosti isporuke SMS poruke – u slučaju da je podešena.
O-97. SMS Gateway mora da podržava

upisivanje, u fajlove i u bazu podataka, zapisa o svakoj poslatoj poruci prema SMS centrima mobilnog operatera sa svim pratećim parametrima koji jednoznačno određuju korišćeni servis (accounting zapisi): vrijeme, SMS centar, servisni i/ili korisnički profil, sadržaj poruke, primaoce i pošiljaoce, notifikacione informacije.
O-98. SMS Gateway mora da podržava telekomunikacioni “back-off” protokol za odloženo slanje SMS poruka u slučaju trenutne nemogućnosti SMS centra mobilnog operatora da primi poruku za dalje slanje. “back-off” protokol predviđa da svaki naredni pokušaj slanja poruke se odlaže za dodatno vrijeme, kako bi se izbjegla eventualna zagušenja, a nakon predviđenog broja iteracija dolazi do trajnog prekida procesa.
O-99. SMS Gateway mora da podržava privremeno čuvanje u trajnom storage prostoru (hard disk) svih prihvaćenih a neisporučenih SMS poruka i notifikacija, za oba pravca, ka SMS centru ili ka korisničkim servisima, sve do konačne isporuke – “Queue” sa predefinisanim vremenom trajanja pokušaja za poruke koje ne mogu biti trenutno obrađene.
O-100. SMS Gateway mora da podržava ograničavanje brzine protoka SMS poruka (broj poruka u sekundi) za svaku konekciju prema SMS centru mobilnog operatora pojedinačno, kao i logovanje trenutnog protoka u sistemskom logu u cilju formiranja istorije iskorišćenosti kapaciteta.
O-101. SMS Gateway mora da podržava slanje i primanje poruka sa ASCII i UNICODE formatom zapisa sadržaja SMS poruke, kao i opciju tekstualnog formata pošiljaoca.
O-102. SMS Gateway mora da podržava podešavanje kratkih kodova i preusmjeravanje dolazećih SMS poruka pema korisničkim servisima na osnovu prve riječi iz sadržaja SMS poruke, kao i da omogućava mehanizam da se odgovori na tako prispjele poruke vrate prema krajnjem korisniku preko istog SMS centra mobilnog operatora sa kojeg su došle.
O-103. SMS Gateway mora da podržava grupno slanje SMS poruka na način da se isti sadržaj poruke pošalje na sve brojeve iz tekstualnog fajla. Grupno slanje poruka se

aktivira ručno od strane administratora sistema.
O-104. SMS gateway mora da omogući konfigurisanje univerzalne HTTP URL adrese za slanje poruka u formatu: http://[adresa servera]:[port]/1.0/sendsms/[brojTelefona]. [brojTelefona] – broj telefona na koji se šalje sa prefikom +382. “Query” http parametri su: [text] – sadržaj sms poruke, [token] – sigurnosni token iz korisničkog profila.
I-44. Tipične aktivnosti prvog nivoa podrške za SMS gateway su: podešavanje korisničkih profila, konekcija prema mobilnim operatorima, pregled accounting zapisa.
I-45. Za implementaciju svih navedenih tehničkih zahtjeva SMS gateway-a su predviđene virtuelne mašine, prema specifikaciji virtuelizovanih resursa iz tenderske dokumentacije.
2.4.12 Crypto sistem
I-46. Naručilac obezbjeđuje HSM modul na kojem su smješteni privatno/javni ključevi osnovnih sertifikacionih tijela sa x509 sertifikatima i AES-256 domenski ključ. Za komunikaciju sa HSM modulom se koristi PKCS11 interfejs. Parametri za povezivanje na HSM modul su: drajver, slot, PIN, identifikacione labele objekata (privatno/javni ključ, x509 sertifikat, AES ključ). Takođe, naručilac definiše dodatne AES-GCM autentifikacione parametre u skladu sa upotrebom. Svi parametri će biti dostupni u momentu konfigurisanja sistema. Sve strukture za skladištenje i razmjenu binarnih informacija (enkriptovanih ili binarno formatiranih) moraju biti otvorenog tipa tj. učitavanje podataka mora biti uvijek moguće nezavisno od ponuđenog rješenja - prateći opisane mehanizme, protokole i standarde.
O-105. Sistem mora da podržava kriptografske funkcije za generisanje AES-256 ključeva i enkripciju/dekripciju podataka po AES-GCM algoritamu (vektor dužina 96 bita, uporedna tag dužina 128 bita) uz dodatne autentifikacione parametre - naznačeni algoritam. Naznačeni algoritam mora uvijek da se koristi u procesima gdje se predviđa enkripcija/dekripcija informacija (ukoliko drugačije nije traženo), a krajnji rezultat enkripcije (enkriptovani fajlovi, enkriptovani odgovori od webservisa,

enkriptovani podaci, enkriptovani ključevi i sl.) mora da bude strukturno formatiran tako da se prvo upiše korišćeni vektor inicijalizacije, odmah u nastavku da slijedi enkriptovani sadržaj, tek na kraju da se upiše tag, dok enkriptovan sadržaj može da ima i svoju strukturu organizacije podataka tj. format.
O-106. Sistem mora da omogućava hijerarhiju AES ključeva, kao i mjesto poziva kriptografskih operacija (na HSM modulu ili van modula), na način: I nivo - domenski i posrednički ključ, II nivo - klijentski ključevi i III nivo - omotni ključevi; Domenski ključ i kriptografske operacije na HSM modulu se koriste za kreiranje/enkripciju/dekripciju posredničkog ključa. Posrednički ključ se koristi za enkripciju/dekripciju klijentskih ključeva i pratećih informacija u vezi sa servisom gdje se koriste klijentski ključevi. Klijentski ključevi se koriste za enkripciju/dekripciju podataka i za enkripciju/dekripciju omotnih ključeva. U radu sa klijentskim i omotnim ključevima se koriste kriptografske operacije isključivo van HSM modula (nije potrebno prisustvo HSM modula).
O-107. Sistem mora da podržava generisanje AES-256 posredničkog ključa. Posrednički ključ mora da se skladišti u jednom fajlu na disku, gdje fajl mora biti enkriptovan koristeći domenski ključ sa HSM modula i zasebno podešene dodatne autentifikacione parametre, sve po naznačenom algoritmu. Posrednički ključ se učitava isključivo prilikom starta sistema uz prisustvo HSM modula i ostaje učitan sve do narednog (re)starta sistema.
O-108. Sistem mora da podržava generisanje AES-256 klijentskih ključeva i da podržava mehanizam rotacije klijentskog ključa. Entitet klijentskog ključa mora da sadrži osnovne podatke (Meta) i inkrementalne verzije sirovog AES-256 ključa (Verzije). Meta podatak mora da uključuje: jedinstveni identifikator (na primjer: c3c0600a-e0aa-4a47-8882-e09a1134ed00) po UUIDv4 (ID), datum kreiranja po RFC3339 (Datum), deskriptivni opis (Opis) i indikator trenutne validnosti ključa (Validan). Verzija ključa mora da sadrži broj koji se uvećava (Inkrement) i sirovi AES-256 ključ (Kljuc). Mehanizam

rotacije podrazumjeva generisanje novog AES-256 sirovog ključa uz povećanje inkrementa verzije za 1. Aktuelna verzija ključa je ona sa najvećim inkrementom. Klijentski ključ mora da se skladišti u jednom fajlu na disku, sa binarnim zapisom po 'Protocol Buffers' (proto3) mehanizmu za serijalizaciju struktuiranih podataka, sa sljedećom definicijom zapisa "message KlijentskiKljuc{MetaPodatak Meta=1;repeated Verzija Verzije=2;} message MetaPodatak{string ID=1;string Datum=2;string Opis=3;bool Validan=4;} message Verzija{int64 Inkrement=1;bytes Kljuc=2;}", gdje fajl mora biti enkriptovan koristeći posrednički ključ i podešene dodatne autentifikacione parametre, sve po naznačenom algoritmu.
O-109. Sistem mora da omogućava webservis pozive za enkripciju/dekripciju podataka pomoću klijentskog ključa. Za proces enkripcije, sistem mora da uvijek koristi aktuelnu verziju klijentskog ključa. Argumenti poziva webservisa za enkripciju podataka uključuju  podatak koji treba enkriptovati, identifikator klijentskog ključa i dodatni autentifikacioni parametar, a odgovor uključuje enkriptovani sadržaj. Enkriptovani sadržaj se sastoji od dvije enkriptovane informacije i mora biti formatiran strukturno tako da sadrži prvo enkriptovan pokazivač korišćenog klijentskog ključa, a u nastavku da se nalazi enkriptovani podatak. Pokazivač  klijentskog ključa se enkriptuje sa posredničkim ključem i formatiran je strukturno na način da prvo sadrži jedinstveni identifikator klijentskog ključa, zatim, separator karakter '#', i na kraju uvijek petocifrenu verziju ključa (nule se dodaju na početak verzije kao dopuna do pet cifara). Argumenti poziva webservisa za dekripciju podataka uključuju enkriptovani sadržaj (nastao ranije u procesu enkripcije) i dodatni autentifikacioni parametar, a odgovor uključuje  dekriptovani podatak.
O-110. Sistem mora da omogućava webservis poziv za ponovnu enkripciju već enkriptovanog podatka sa drugim ključem (zamjena klijentskog ključa). Argumenti poziva webservisa uključuju enkriptovani sadržaj, identifikator novog klijentskog ključa i dodatni autentifikacioni parametar, a odgovor uključuje novoenkriptovani sadržaj.

O-111. Sistem mora da omogućava webservis za generisanje AES-256 omotnog ključa. Argumenti poziva webservisa uključuju identifikator klijentskog ključa i dodatni autentifikacioni parametar, a odgovor webservisa uključuje sirovi omotni ključ i enkriptovani sadržaj sa omotnim ključem. Za dekripciju sadržaja sa omotnim ključem se koristi specificirani webservis za dekripciju podataka. (Omotna kriptografija podrazumjeva enkripciju/dekripciju podataka koja se izvršava na strani klijenta, a sistem se koristi samo za generisanje jednokratnih (ne skladište se na strani sistema) omotnih ključeva. Sirovi omotni ključ se uništava po okončanju procesa enkripcije/dekripcije podatka na strani klijenta.)
O-112. Sistem mora da podržava automatsko rotiranje klijentskih ključeva na godišnjem nivou, tako da se u naznačenom intervalu generiše novi AES ključ (nova verzija klijentskog ključa) koji važi od tog momenta, ali tako da je moguće sprovesti dekripciju podataka koji su enkriptovani sa nekom od prethodnih verzija klijentskog ključa, a sve u skladu sa formatom entiteta klijentskog ključa.
O-113. Rješenje mora da omogućava CLI alat, na ponuđenoj Linux distribuciji, koji obavlja enkripciju/dekripciju fajlova po AES-CTR algoritmu ('all-zero' vektor inicijalizacije) koristeći zasebno generisani omotni ključ za svaki fajl pojedinačno, sa neophodnim okvirom komandnih argumenata i koristeći samo potrebne webservise za omotnu kriptografiju. Enkriptovani sadržaj sa omotnim ključem, kao i sami enkriptovani fajl, moraju da se smještaju u zasebnim fajlovima sa predefinisanim nazivom - tako što se na naziv originalnog fajla dodaje sufiks ".key" ili ".encrypted" u zavisnosti da li se radi, redom, o enkriptovanom ključu ili enkriptovanom fajlu.
O-114. Rješenje mora da omogućava CLI alat, na ponuđenoj Linux distribuciji, koji obavlja 'offline' dekripciju fajlova (na nezavisnim serverskim mašinama van mreže) po AES-CTR algoritmu ('all-zero' vektor inicijalizacije) koristeći omotni ključ, sa neophodnim okvirom komandnih argumenata, gdje je lokalno na serverskoj mašini dostupan samo HSM modul, posrednički ključ, odgovarajući klijentski

ključ, enkriptovani omotni ključ i enkriptovani fajl. (Parametri za rad sa HSM modulom i dodatni autenfikacioni parametri se zadaju u momentu korišćenja CLI alata.)
O-115. Sistem mora da podržava import fajlova koji sadrže ključeve (posrednički i klijentski ključevi) na način da je dovoljno samo kopirati fajlove u odgovarajući direktorijum i opcionalno restartovati sistem, nakon čega odmah mora da bude moguća njihova upotreba.
O-116. Sistem mora da podržava rad sa više osnovnih sertifikacionih tijela (RootCA) sa HSM modula (u skladu sa odgovarajućim pristupnim parametrima), kao i upravljanje kriptografskim operacijama sa HSM modula u procesima generisanja i potpisivanja sertifikata.
O-117. Sistem mora da podržava kreiranje više posredničkih sertifikacionih tijela (Intermediate CA), tako što će posrednički CA sertifikati biti potpisani od strane odabranog osnovnog sertifikacionog tijela sa HSM modula, a privatni ključ od posredničkog sertifikacionog tijela mora biti smješten na disku u enkriptovanom fajlu po naznačenom enkripcionom algoritmu (koristeći pridruženi klijentski ključ od nadležnog posredničkog CA).
O-118. Sistem mora da podržava generisanje x509 sertifikata sa 2048 i 4096-bitnim RSA ključevima i ECDSA ključevima sa krivim P-224, P-256, P-384 i P-521. Privatni ključevi se u sistemu mogu skladištiti isključivo enkriptovano po naznačenom enkripcionom algoritmu koristeći pridruženi klijentski ključ od nadležnog posredničkog CA.
O-119. Sistem mora da podržava potpisivanje sertifikata sa posredničkim sertifikacionim tijelom (posrednički CA), gdje su sertifikati generisani unutar sistema, kao i potpisivanje po zahtjevu za potpisivanje sertifikata (CSR zahtjev) i da podržava digitalne potpise SHA-128, SHA-256, SHA-384, SHA-512.
O-120. Sistem mora da podržava eksport potpisanog sertifikata (prethodno generisan u sistemu), odgovarajućeg privatnog ključa, kao i CA lanca (osnovni+posrednički), sve zajedno u p12 formatu. Sistem mora da omogućava eksport bilo kojeg pojedinačnog sertifikata u PEM formatu.

O-121. Sistem mora da podržava podešavanje više PKI (Public Key Infrastructure) profila sa proizvoljnim elementima koji su potrebni za ažuriranje x.509 sertifikata (kombinacija ekstenzija za posebne namjene x.509 sertifikata).
O-122. Sistem mora da podržava OCSP serverske tačke (endpoint) u cilju provjere validnosti sertifikata od strane udaljenih klijenata, kao i da se predviđene OCSP putanje upisuju u sertifikat.
O-123. Sistem mora da omogućava upravljačko rješenje zasnovano na web tehnologijama tako da je na klijentskoj strani dovoljno koristiti samo web browser u cilju rada sa grafičkim korisničkim interfejsom, sve tako da podržava izvršenje tipičnih dnevnih aktivnost prvog nivoa podrške. Upravljačko riješenje mora imati razdvojenu komponentu baze podataka sa omogućenim zasebnim pristupom za DB administratora.
O-124. Upravljačko rješenje mora da podržava softverski modul za svu neophodnu administraciju sistema. (na primjer: unos korisnika, podešavanja prava i privilegija i sl.).
O-125. Upravljačko rješenje mora da podržava multikorisničko okruženje gdje se za pristup sistemu koristi autorizacija sa korisničkim nalogom i lozinkom.
O-126. Upravljačko rješenje mora da podržava sistem prava i privilegija koje se preko konfigurabilnih rola dodijelju korisnicima sistema. Prava i privilegije generički moraju da obuhvataju podešavanje definicija za pristup softverskim modulima (cjeline administracija i kriptografija), određenim stranicama unutar modula (generisanje klijentskih ključeva, sertifikata i sl.), ključnim entitetima (korisnik, sertifikat, klijentski ključ i sl.), atributima entiteta (datum generisanja, ime, prezime, opis i sl.) i specifične privilegije. Specifične privilegije obuhvataju: pravo za generisanje posredničkih sertifikacionih tijela, pravo za potpisivanje sertifikata, pravo za eksport sertifikata, pravo za generisanje klijentskih AES ključeva, pravo pristupa REST web servisima, pravo pristupa grafičkom korisničkom interfejsu, pravo pristupa korisničkom interfejsu interaktivne dokumentacije web servisa.
O-127. Upravljačko rješenje mora da

podržava definisanje proizvoljnih logičkih kombinacija uslova filtera za pretragu ključnih entiteta iz modela.
O-128. Upravljačko rješenje mora da podržava eksport podataka u Excel formatu uz svaku tabelu koja prikazuje atribute entita iz modela, pri čemu korisnik može sam da označi kolone, redosled kolona i redove koji će biti eksportovani. Za označavanje redova, korisnik može da koristi kombinacije logičkih uslova filtera pretrage, i to sve kroz više korisničkih iteracija zadavanja upita pretrage dok ne formira željenu selekciju podataka za eksport.
O-129. Upravljačko rješenje mora da podržava upis svih vremenskih podataka u bazi podataka sa vremenskom zonom UTC i da potrebne mehanizme rada sa vremenskim zona realizuju unutar aplikacije, tako da promjena vremenske zone na samom operativnom sistemu servera nije od uticaja na već upisane vremenske podatke u bazi podataka.
O-130. Upravljačko rješenje mora da podržava praćenje i trajno čuvanje svih izmjena nad entitetima modela i pripadajućim relacijama, kao i praćenje obrisanih podataka, u svrhu sigurnosnog traga (“audit trail”). Svaki zapis praćenja mora jasno da ukazuje na atribute entiteta koji su izmjenjeni, uz podatke o vremenu, koji korisnik je izvršio izmjenu, i porijeklu izmjene (grafički korisnički interfejs ili REST web servis). Svaki od entiteta pojedinačno mora da sadrži podatke o vremenu i korisniku koji je prvi put kreirao entitet modela, kao i zadnji put izmijenio entitet modela. Pristup ovim informacijama mora biti omogućen nezavisno od korisničkog interfejsa aplikacije.
O-131. Upravljačko rješenje mora da podržava integraciju sa trećim sistemima preko REST web servisa. Za pristup REST web servisima od strane trećih sistema se koristi mehanizam autorizacije preko korisničkog naloga i lozinke, koji se ujedno mogu koristiti i za pristup grafičkom korisničkom interfejsu. Za korisnike web servisa iz trećih sistema, a nakon uspješne autentifikacije, se prvo registruje sesija tako da za sve naredne pozive web servise nije potrebna ponovna autentifikacije već se uz poziv proslijeđuje samo indikator sesije.

O-132. Upravljačko rješenje mora da podržava prepoznavanje indikatora korisničke sesije iz predefinisanog nezavisnog atributa iz zaglavlja (hedera) i iz “Cookie”-a  HTTP zahtjeva. Klijentska strana može ravnopravno da koristi ili jedan ili drugi mehanizam smještanja indikatora korisničke sesije u HTTP zahtjevu.
O-133. Upravljačko rješenje mora da podržava interaktivnu dokumentaciju REST web servisa, gdje se opis poziva nalazi kao dio integrisan u okviru grafičkog korisničkog interfejsa (sastavni dio administratorskog modula aplikacije) zajedno sa mogućnošću poziva uživo - preko forme u okviru koje se popunjavaju parametri poziva tog web servisa.
O-134. Upravljačko rješenje mora da podržava administratorske opcije za odjavu svih korisnika (logout all), slanje poruka svim korisnicima (broadcast), pregled svih aktivnih korisničkih sesija grafičkog korisničkog interfejsa i web servisa. Pregled mora da uključuje vrijeme zadnje aktivnosti korisnika. Broadcast poruke se prikazuju u svim browser prozorima ulogovanog korisnika i blokiraju korisnički interfejs sve dok korisnik ne zatvori poruku. Opcija za odjavu svih korisnika se izvršava odmah bez ikakvog korisničkog upozorenja, ali tako da ne izloguje administratora koji je pokrenuo odjavu svih korisnika.
O-135. Upravljačko rješenje mora da podržava višejezičko okruženje grafičkog korisničkog interfejsa, tako da obezbijeđuje mogućnost podešavanje jezika za pojedinačnog korisnika kroz administratorski interfejs. Upravljačko rješenje mora da obezbijeđuje opciju za Crnogorski (default) i Engleski jezik.
O-136. Upravljačko rješenje mora da podržava istorijske zapise svih korisničkih sesija, koje moraju imati sledeće atribute entiteta: jedinstveni identifikator sesije, IP adresa, vrijeme početka i kraja sesije, tip sesije (grafički korisnički interfejs ili web servis sesija), korisnik, i opisne informacije klijentskog web browsera.
O-137. Softversko rješenje mora da podržava automatski dnevni backup svih podataka i odlaganje u trajnu arhivu na udaljenom serveru preko SCP ili FTP protokola.

O-138. Upravljačko rješenje mora da podržava klasterizovanu implementaciju. Implementacija mora da obezbijeđuje: dostupnost svih relevantnih komponenti u slučaju ispada nekog od nodova u klasteru; skalabilnost čitanja iz baze podataka; skalabilnost aplikativne logike sa dodavanjem novih odgovarajućih komponenti u klaster; raspoređivanje novih korisničkih sesija u odnosu na 5-minutno prosječno zauzeće procesora da bi se postiglo adekvatno iskorišćenje predviđenih kapaciteta. U slučaju ispada, toleriše se gubitak uspostavljenih sesija samo sa nedostupnog noda.
O-139. Ponuđač mora da obezbijedi razvojnu podršku u periodu do 30 dana za eventualne dodatne manje izmjene i prilagođavanja na sistemu kako bi Naručilac bolje upodobio sistem prema svojim potrebama.
I-47. Tipične aktivnosti prvog nivoa podrške za sistem su: generisanje, pretraga, poništavanje i eksport sertifikata (korisničkih sertifikata i posredničkih CA tijela), ažuriranje baze poništenih sertifikata, generisanje AES ključeva, podrška u radu sa web servisima, enkripcija/dekripcija fajlova na strain drugih sistema.
I-48. Za implementaciju svih navedenih tehničkih zahtjeva Crypto sistema su predviđene virtuelne mašine, na način da su serverski razdvojene ključne logičke funkcionalnosti (upravljački interfejs / aplikacija, HSM kriptografske operacije, verifikacija certifikata / OCSP tačka), prema specifikaciji virtuelizovanih resursa iz tenderske dokumentacije.
2.4.13 Trustpoint sistem
O-140. Trustpoint  rješenje mora da podržava terminaciju SSL/TLS enkriptovanih konekcija preko HTTP 1.1 i 2.0 protokola (https konekcije), kao i WebSocket-a sa udaljenih lokacija (preko http-upgrade mehanizma), i njihovo preusmjeravanje prema unutrašnjim servisnim URL putanjama (po principu balansiranja).
O-141. Trustpoint  rješenje mora da podržava podešavanje HTTPS endpoint-a sa unutrašnjim servisnim URL putanjama uz mogućnost definisanja zasebnog x509 sertifikata po endpoint-u i autentifikaciju

udaljenih lokacija sa zasebnim CA sertifikatom.
O-142. Trustpoint rješenje mora da podržava osnovnu autentifikaciju udaljenih lokacija po modelu korisničkog naloga i lozinke po http protokolu.
O-143. Trustpoint rješenje mora da podržava preusmjeravanja dolaznog endpoint saobraćaja prema unutrašnjim URL putanjama u skladu sa predefinisanim algoritmom: round-robin, least connection i hashing po parametrima iz HTTP zahtjeva. Algorimi za balansiranje moraju da podržavaju opciju za 'sticky' sesije (na osnovu cookie-a) tako da aktivna sesija završava uvijek na istu unutrašnju URL putanju gdje je i prvi put uspostavljena.
O-144. Trustpoint rješenje mora da podržava fail-over između unutrašnjih URL putanja, gdje u slučaju ispada, dolazana konekcija se preusmjerava prema narednoj ispravnoj lokaciji u skladu sa algoritmom za balansiranje.
O-145. Trustpoint rješenje mora da podržava provjere ispravnosti (health check) unutrašnjih URL putanja u predefinisanim vremenskim intervalima po HTTP protokolu, na proizvoljnoj URL putanji i portu, za svaku unutrašnju putanju pojedinačno, na način da provjera statusni kod odgovora sa strane konkretnog servisa uz odgovarajuće maksimalno vrijeme čekanja (timeout).
O-146. Trustpoint rješenje mora da u slučaju pojave učestanih neispravnosti unutrašnjih servisa u predviđenom vremenskom intervalu isključi problematičnu unutrašnju putanju na određeno vrijeme, bez obzira što ona za neke zahtjeve prethodno ponekad vraća ispravne odgovore. (mogućnost dodatnog vremena za eventualnu stabilizaciju servisa).
O-147. Trustpoint rješenje mora da podržava visoko-dostupne (High Availiability - HA) implementacije. U slučaju ispada nekog od nodova u klasteru, toleriše se ponovno uspostavljanje konekcija i identifikacija udaljenih lokacija.
O-148. Trustpoint rješenje mora da podržava servisne http pristupne liste (access list) za svaku od unutrašnjih putanja pojedinačno, po svim tipovima http zahtjeva (GET, POST, DELETE itd.) i unutrašnjoj URL putanji.

O-149. Trustpoint rješenje mora da obezbjeđuje konfiguraciju SSL/TLS protokolnih parametara u skladu sa vodećim sigurnosnim preporukama, tako da na online Internet testu (Qualys SSL Labs - SSL Server test)  ne smije da dobije manju ocijenu od “A”. Online adresa preko koje se testira je: https://www.ssllabs.com/ssltest/
O-150. Trustpoint rješenje mora da podržava osnovni i napredni set firewall/ruter mrežnih funkcionalnosti iz tehničkih zahtjeva.
O-151. Trustpoint rješenje treba da omogućava administratorski interfejs/alat, ili konfiguracione fajlove, na način da podržava izvršenje tipičnih dnevnih aktivnost prvog nivoa podrške.
I-49. Tipične aktivnosti prvog nivoa podrške za ovaj sistem su: podešavanje unutrašnjih putanja i endpoint-a, ažuriranje mrežnih ruta, pregled logova, podešavanje x509 i drugih sigurnosnih parametara.
I-50. Za implementaciju svih navedenih tehničkih zahtjeva Trustpoint sistema su predviđene virtuelne mašine, prema specifikaciji virtuelizovanih resursa iz tenderske dokumentacije.
2.4.14 SDS sistem (Software-Defined-Storage)
O-152. SDS sistem mora da omogućava visoko-skalabilno klasterizovano skladište za smještanje fajlova, objekata i blokova podataka (block disk) na način da sastavni softverski slojevi omogućavaju nezavisnost od posebno specijalizovanog hardvera.
O-153. SDS sistem mora da omogućava pozadinsko ravnomjerno distrubuiranje podataka unutar klastera, kontinuiranu pozadinsku provjeru integriteta podataka i samostalni oporavak u slučaju ispada.
O-154. SDS sistem mora da omogućava nadogradnju softvera u fazama bez ili sa minimalnim vremenom prekida rada klastera.
O-155. SDS sistem mora da podržava protokole AWS S3 i Swift za rad sa objektima, integracione mehanizme sa KVM hipervizorima za virtuelizaciju diska od virtuelnih mašina, integraciju sa standardnim Linux-zasnovanim fizičkim serverima za rad sa blokovima podataka (pridruženim diskom) preko mreže i POSIX-kompatibilni klasterizovani fajl sistem (dijeljiv pristup ka

fajl sistemu između više klijenata).
O-156. SDS sistem mora da omogućava grafički interfejs za monitoring i dijagnostiku sistema, uključujući statistiku korišćenja za čitav klaster i pojedinačno po komponentama.
O-157. SDS sistem mora da omogućava kontrolu pristupa za korisnike sistema po nivoima smještenih podatka (na primjer: ‘pools’, ‘object buckets’, putanje ka fajlovima i sl).
O-158. SDS sistem mora da omogućava enkripciju objekata na osnovu proslijeđenih kriptografskih ključeva u zahtjevu bez ikakve specijalne konfiguracije na sistemu da bi se podržao ovaj enkripcioni režim.
O-159. SDS sistem mora da omogući adekvatnu algoritamsku zaštitu dugoročnosti podataka uz podržanu visoku dostupnost podatka i visoke performanse pri radu sa podacima, a sve uz odgovarajuću ekonomičnost u pogledu smještajnih kapaciteta.
O-160. SDS sistem mora da omogućava proširenje ili smanjenje blokova podataka bez prekida u radu sistema (downtime).
O-161. SDS sistem mora da omogućava podešavanja polisa za smještanje podataka u skladu sa performansnim zahtjevima, odgovarajućom skladištenom lokacijom (na primjer: sporiji ili brži diskovi za smještanje podataka) i domenima mogućih ispada (na primjer: rack ormar, ili spratnost data centra).
O-162. SDS sistem mora da omogućava momentalne snimke blokova podataka (snapshots) bez prekida u radu sistema ili značajnih penala po performanse i odziv sistema u datom momentu.
O-163. SDS sistem mora da omogućava distribuciju klijentskih konekcija za prenos podataka preko cijelog klastera na način da ne postoji pojedinačna tačka mogućeg ispada u komunikaciji (single point of failure).
O-164. SDS sistem mora da omogućava kloniranje blokova podataka na način da se od jednog bloka podataka može momentalno izdvojiti brojne kopije nezavisnih blokova podataka, bez prekida u radu sistema ili značajnih penala po performanse i odziv sistema u datom momentu.

O-165. SDS sistem mora da omogućava implementaciju finog podešavanja za veće performanse pri upisivanju podataka kroz odgovarajuće žurnaling/kešing tehnologije.
O-166. SDS sistem mora da podržava replikaciju objekata između lokacija i automatsko arhiviranje verzija objekata.
O-167. SDS sistem mora da omogućava dimenzioniranje blokova podataka na način da ukupna veličina tek kreirianog bloka može da prelazi veličinu instalisanih kapaciteta (thin provisioning).
O-168. SDS sistem mora da omogućava replikaciju blokova podataka na udaljenu DR (disaster recovery) lokaciju. SDS sistem mora da omogućava automatizovani mehanizam za backup objekata po BACKUP-3-2-1 pravilu – najmanje tri kopije podataka, barem dva različita medijuma za smještanje, gdje jedna kopija mora biti van glavne lokacije.
O-169. BACKUP-3-2-1 sistem mora da uključuje implementaciju primarnog SDS sistema, sa kojeg se prenose podaci prema backup SDS sistemu, sa kojeg se preuzimaju podaci inicirano sa backup servera povezanog na biblioteku traka. Za vezu između backup servera i SDS sistema za prenos podataka potrebno je implementirati HPS (high-performance switching) gateway na SDS sisteme (standardni mrežni saobraćaj se sa jedne strane rutira prema uređajima za visoko-performantni switching unutar SDS sistema). U okviru BACKUP-3-2-1 sistema moraju biti implementirani procesi za izradu rezervnih kopija podataka i automatizovanu rotaciju traka (automatizovano snimanje nastavlja na narednu traku sve do iskorišćenja zadnje trake, kada sistem nastavlja ponovo da snima počev od prve trake) i to procesi: automatizovano za sve logičke rezervne kopije sa predviđenih lokacija skladišta objekata na dnevnom nivou na zasebnom rotacionom pool-u traka; za sve rezervne kopije slika blokova podataka (na zahtjev) na zasebnom rotacionom pool-u traka; za izradu šifriranih rezervnih kopija (na zahtjev) na trake koje se odlažu van zgrade. Na kraju svakog pokrenutog procesa za izradu rezervnih kopija na trake potrebno je na backup serveru čuvati do dvije godine sve izvještaje, kao i slati te izvještaje na

predefinisane mejl adrese. Izvještaji moraju minimalno da uključuju identifikator rezervne kopije, nazive datoteka ili druge reference koje su ušle u datu rezervnu kopiju, serijski broj trake, redni broj arhive na traci i prostorno zauzeće napravljene rezervne kopije na traci. Pravo/privilegije za pokretanje procesa za izradu rezervnih kopija na sistemu mora biti dodijeljeno samo određenim korisnicima na način da ti korisnici ne mogu ništa drugo da izvrše na sistemu (isključuvo pokretanje procesa za izradu rezervnih kopija, bez mogućnosti izvršavanja bilo koje druge komande na sistemu). Nakon implementacije je potrebno dostaviti dokumentovane procedure za izradu i oporavak podataka sa traka na osnovu implementiranih procesa u skladu sa datim opisima, kao i proceduru za generisanje novog ključa za šifrovanje podataka.
O-170. SDS rješenje treba da omogućava administratorski interfejs/alat, ili konfiguracione fajlove, na način da podržava izvršenje svih administratorskih aktivnosti.
I-51. Za implementaciju svih navedenih tehničkih zahtjeva SDS sistema su predviđene fizičke mašine, prema specifikaciji hardverskih resursa iz tenderske dokumentacije. Za sistem backupa podataka su predviđeni resursi za implementaciju zasebnog backup SDS sistema (pored produkcionog SDS sistema), kao i nezavisni backup server na izdvojenoj lokaciji van glavne lokacije (BACKUP 3-2-1 pravilo), biblioteka za trake i server za implementaciju HPS gateway-a.
3. SPECIFIKACIJA PRODUKCIONOG I POMOĆNOG HARDVERA I VIRTUELIZOVANIH RESURSA
3.1. Hardver i virtuelizovani resursi predviđeni za produkciono okruženje

Hardver sa sledećom specifikacijom:
- Firewall/Ruter
HP DL360G10, Intel (R) Xeon Gold (R) CPU 6144 3,5 GHz, 2 CPU, 8 cores, 2x300 GB HDD, 32 GB RAM, 1Gb Ethernet 4-port Adapter, 10Gb/40Gb 2-port +QSFP Adapter, 2 napajanja.
HP DL360G10, Intel(R) Xeon(R) Silver 4114 CPU @ 2.20GHz, 2 CPU, 10 cores, 2x300

GB HDD, 32 GB RAM, 1Gb Ethernet 4-port Adapter, 10Gb/40Gb 2-port +QSFP Adapter, 2 napajanja;
- Platforma za virtuelizaciju
Hipervizori :
(povezani na SDS sistem)
7 x (HP DL360G10, Intel (R) Xeon (R) Gold CPU 5122 3.6 GHz, 2 CPU,  4 cores, 2 threads per core, 2x900 GB SAS, 256 GB RAM, 4x10Gbps NIC, 1Gb Ethernet 4-port Adapter, 2 napajanja)
Podrška migraciji fizičkih računara u gost virtuelne mašine :
1x DL360G10 ,Intel (R) Xeon Gold (R) CPU 5122 3.6 GHz, 2 CPU,  2x600GB HDD, 64GB RAM, 4x10Gbps NIC, 4x1Gbps NIC.
- SDS sistem
11x DL360G10 ,Intel (R) Xeon Gold (R) CPU 6248 2.5 GHz, 2 CPU,  2x600GB HDD, 192GB RAM, 2x10Gbps NIC, 2x40Gbps NIC, 4x1Gbps NIC , 4x3.5TB SSD, 1x750GB NVMe SSD
3x DL360G10 ,Intel (R) Xeon Silver (R) CPU 4208 2.1 GHz, 2 CPU,  2x600GB HDD, 64GB RAM, 2x10Gbps NIC, 4x1Gbps NIC
1x DL360G10 ,Intel (R) Xeon Gold (R) CPU 5122 3.6 GHz, 2 CPU,  2x600GB HDD, 64GB RAM, 4x10Gbps NIC, 4x1Gbps NIC
- Backup SDS
5 x (HP DL380G10, Intel (R) Xeon (R) Gold CPU 5122 3.6 GHz, 2 CPU,  4 cores, 2 x 240GB SATA RI M.2 SSD, 10 x 10TB SAS 7.2K LFF SC He 512e DS HDD,  GB RAM, 4x10Gbps NIC, 1Gb Ethernet 4-port Adapter, 2 napajanja)
- Backup Server
1 x (HP DL380G10, Intel (R) Xeon (R) Gold 2.5 GHz, 2 CPU,  10 cores, 7 x 16 TB SATA, 1 x 512 GB SSD , 2 x 128 GB NVMe drives, 128 GB RAM, 7 x HDD 16TB SATA 7.2K LFF SC He 512e DS HDD, 1 x Ethernet 10 GB SFP, 1Gb Ethernet 4-port Adapter, 2 napajanja)

1x TAPE LIBRARY
- Tejp lajbreri uredjaj (uredjaj biblioteke traka) namjenjen za montazu u rek orman, podrska za 48 tejp drajv uredjaja i 640 slotova za trake samostalno ili putem dodatnih modula za nadogradnju Sistema
- tri (3) ugradjena uredjaja traka ("tejp drajv") LTO-9 Ultrium 45000 sa SAS interfejsom
- četrdeset (40) ukljucenih slotova za trake

- HPS  gateway (High-performance switching)
1x (HP DL360G10, Intel (R) Xeon (R) Gold CPU 5122 3.6 GHz, 2 CPU,  4 cores, 2 threads per core, 2x900 GB SAS, 256 GB RAM, 4x10Gbps NIC, 1Gb Ethernet 4-port Adapter, 2 napajanja), povezan sa optičkim kablom direktno na backup server

- TESTNI SERVER
DL360G10 ,Intel (R) Xeon Gold (R) CPU 5122 3.6 GHz, 2 CPU,  2x600GB HDD, 64GB RAM, 4x10Gbps NIC, 4x1Gbps NIC
Virtuelizovani resursi sa sledećom specifikacijom:
- DNS sistem
1 virtuelna mašina: 1 CPU, 1GB RAM, 8GB HDD, 1 NIC.
1 instanca na Internetu (slave): 1 CPU, 1GB RAM, 8GB HDD, 1 NIC, 1x javna IP adresa.
- Proxy sistem
1 virtuelna mašina :1 CPU, 1GB RAM, 10GB HDD, 2 NIC
- VPN platforma
2 virtuelne mašine (4 CPU, 4 GB RAM, 12GB HDD, 2 NIC)
- SSO sistem (Single Sign-on platforma)
do 2 virtuelne mašine  (zbirno: 4 CPU, 4GB RAM, 40GB HDD, 3+ NIC)
- Sistem za mrežni monitoring
1 virtuelna mašina (2 CPU, 4 GB RAM, 30GB HDD, 1+ NIC)
- SSL gateway
1 virtuelna mašina (2 CPU, 4GB RAM, 20GB HDD, 2 NIC)
- SMS gateway
1 virtuelna mašina :1 CPU, 1GB RAM, 20GB HDD, 1 NIC
- Crypto sistem
1 virtuelna mašina: 4 CPU, 8GB RAM, 30GB HDD, 1 NIC
1 virtuelna mašina: 2 CPU, 2GB RAM, 30GB HDD, 1 NIC
1 virtuelna mašina: 2 CPU, 2GB RAM, 30GB HDD, 1 NIC
- Trustpoint sistem
1 virtuelna mašina  (4 CPU, 8 GB RAM, 20GB HDD, 3 NIC)
- Mail sistem
1 virtuelna mašina  (4 CPU, 16 GB RAM, 30GB HDD, 1TB HDD, 2 NIC)

| | | | | | |
|---|---|---|---|---|---|
| | | | 4.2 Predviđeni privremeni hardverski resursi i virtuelne mašine<br>Predviđeni su privremeni hardverski resursi i virtuelne mašine, dostupne do završetka implementacije:<br>- VM serveri za ostalu privremenu upotrebu<br>6 x virtuelna mašina: 2 CPU, 2GB RAM, 8GB HDD, 2+ NIC. | | |

**Tehnička specifikacija nakon izmjena**

| Procijenjena vrijednost bez PDV | Redni broj predmeta nabavke | Opis predmeta nabavke | Bitne karakteristike predmeta nabavke | Količina | Jedinica mjere |
|---|---|---|---|---|---|
| 72000.00 | 1 | Usluga održavanja aplikacija i sistema baziranih na OpenSource tehnologijama:<br>-Usluge implementacije, tehničke podrške i održavanja aplikacija i sistema baziranih na OpenSource tehnologijama u okviru Integralnog informacionog sistema zdravstva Crne Gore | 1. OPŠTI ZAHTJEVI I INFORMACIJE<br>1.1 Generalno<br>I-1. Segmenti FZOCG sistema za koje će ponuđač pružati usluge iz predmeta javne nabavke prema traženim tehničkim i drugim zahtjevima su:<br>• Firewall/Ruter<br>• VPN koncentrator<br>• SSL gateway<br>• Virtuelizacija servera<br>• Mail sistem<br>• Sistem za mrežni monitoring<br>• Proxy sistem<br>• DNS sistem<br>• SSO sistem (Single Sign-on platforma)<br>• VPN klijent<br>• Crypto sistem<br>• SMS gateway<br>• Trustpoint sistem<br>• SDS sistem (Software-Defined-Storage)<br>I-2. Za sve navedene segmente sistema, FZOCG obezbijeđuje raspoložive hardverske resurse i resurse virtuelizovanih mašina prema datoj specifikaciji, koja čini sastavni dio tenderske dokumentacije, zatim, javne IP adrese za potrebe servisa, mrežne i druge infrastrukturne konfiguracije i parametre potrebne za instalaciju, kao i relevantne podatke potrebne za migraciju trenutnog produkcionog okruženja na ponuđena rješenja (firewall pravila, korisničke podatke, mailbox-ove, liste aktivnih profila, parametre profila i sl.) odmah po zaključenju ugovora. | 1.00 | komplet |

FZOCG za sve hardverske resurse obezbijeđuje potrebne infrastrukturne elemente i povezivanja (postavljanje opreme u rack ormaru, dovod napajanja i mrežnih kablova, optičkih veza prema storage sistemu). Zbirni resursi planiranih virtuelizovanih kapaciteta su predviđeni prema grupi virtuelnih mašina zbog fleksibilnosti preraspodjele resursa u trenutku konfiguracije virtuelnih mašina. Potrebno je da ponuđač, u odgovarajućim odgovorima za konkretne sisteme, navede pojedinačne dodjele resursa (cpu, ram, disk i sl.) virtuelnim mašinama, koje planira da iskoristi za potrebe ponuđenih rješenja, tako da zbir dodjeljenih resursa pojedinačnim konfiguracijama virtuelnih mašina ne smije prelaziti ukupan zbir planiranih kapaciteta u datoj specifikaciji.

1.2 Obavezna forma odgovora
I-3. Zahtjevi koji su postavljeni u dokumentu su naznačeni kao:
• O – Obavezan zahtjev: neophodno je da ponuđač dostavi ponudu koja ispunjava zahtjev. Neispunjenjem bilo kojeg obaveznog zahtjeva ponuda se smatra neadekvatnom i odbacuje se.
• P – Poželjan zahtjev: neophodno je da ponuđač dostavi ponudu koja je u skladu sa zahtjevom, ali on nije obavezan (eliminatoran).
• I – informacije i uputstva koje je ponuđač dužan uzeti u obzir i pridržavati ih se prilikom sačinjavanja i podnošenja ponude. Neispunjenjem bilo kojeg uputstva, datim pod ovom naznakom (I), ponuda se smatra neadekvatnom i odbacuje se.
I-4. Ponuđač je dužan da odgovore na sve zahtjeve dostavi u jednoj cjelini, tako da svaki odgovor mora da bude složen po redosljedu sadržaja navedenih tehničkih zahtjeva i da bude povezan sa rednim brojem zahtjeva u odgovoru.
I-5. Uz odgovor na svaki pojedini zahtjev, potrebno je da ponuđač jasno stavi naznaku koja predstavlja izjavu o stepenu podržanosti, koristeći sljedeće norme kvalifikacije: u potpunosti podržano (P), djelimično podržano (D). Ukoliko se ponuđač za neki od zahtjeva ne izjasni stepenom podržanosti, ponuda se smatra neadekvatnom i odbacuje se.

I-6. (P) – označava da su, u predloženim rješenjima, svi zahtjevi podržani bez poznatog tehničkog ograničenja.
I-7. (D) – označava da je zahtjev podržan uz određena tehnička odstupanja i ograničenja. Tehnička odstupanja i ograničenja moraju biti opisana i posebno objašnjena u odgovoru.
I-8. Neophodno je da ponuđač u odgovoru na svaki tehnički zahtjev, dostavi dovoljno informacija vezano za tehničke detalje predloženih rješenja i relevantne tehničke standarde, na način da se iz odgovora može od strane FZOCG utvrditi osnovna tehnička izvodjlivost traženog zahtjeva u ponuđenom riješenju u skladu sa svim ostalim datim instrukcijama i uputstvima. Ponuda koja ne sadrži dovoljno informacija za evaluaciju smatraće se neadekvatnom i odbacuje se.
2. TEHNIČKE KARAKTERISTIKE I SPECIFIKACIJE
2.1 Opšti zahtjevi
O-1. Ponuđač je dužan navesti operativne sisteme (OS) koje koristi u ponuđenim rješenjima. Operativni sistem mora biti namjenjen za serverska okruženja i mora da podržava standardni mehanizam u cilju softverske nadogradnje i zakrpe. U slučaju naknadnog nastanka nemogućnosti nadogradnje ili zakrpe ponuđač je dužan da na zahtjev predloži drugo kompatibilno rješenje i izvrši potrebne aktivnosti implementacije tog rješenja.
O-2. Ponuđeni operativni sistem mora da podržava mehanizam za automatsku instalaciju i konfiguraciju operativnog sistema bez interakcije administratora u toku instalacionog procesa. Potrebno je navesti preduslove koje FZOCG treba da obezbijedi za slučaj korišćenja ovog mehanizma.
I-9. Ponuđač je dužan ponuditi implementaciju, održavanje i tehničku podršku za sva ponuđena rješenja. Usluge implementacije, između ostalog, obuhvataju i eventualnu privremenu instalaciju i konfiguraciju ponuđenih rješenja u cilju preuzimanje postojećeg produkcionog okruženja na održavanje, zatim, migraciju podataka i integraciju sa ostalim IT okruženjem.
I-10. Ponuđač je dužan ponuditi arhitekturu rješenja, koja se zasniva na OpenSource tehnologijma, na način da ne postoje

nikakva ograničenja po pitanju uslova licenciranja po parametrima okruženja (kao npr. po broju istovremenih konekcija, broju korisnika, broju procesora, broju lokacija i sl.) i u slučaju prekida saradnje sva prava korišćenja za sve sisteme moraju ostati u vlasništvu FZOCG za neograničenu internu upotrebu u okviru Integralnog informacionog sistema zdravstva.
I-11. Sva ponuđena riješenja, u okviru redudantnih/klaster cjelina pojedinačnih sistemskih segmenata, moraju biti jednobrazna po pitanju izbora tehnologija, odnosno nije dozvoljeno korišćenje jedne tehnologije na jednom klaster nodu, dok na drugom nodu u istom klasteru da se koristi druga tehnologiju za realizaciju istog servisa za koji je predviđen taj klaster. Takođe, u konačnoj implementaciji, sve verzije softvera i konkretne softverske komponente moraju biti iste na svim klaster nodovima, na način da se nodovi razlikuju samo u podešavanjima.
I-12. Ponuđač ne smije unazaditi sistem po pitanju softverskih verzija, odnosno koristiti verzije softvera starije od onih koje standardno dolaze uz instalaciju operativnog sistema ili od onih verzija koje su dostupne kroz standardni kanal softverske nadogradnje (onaj kanal koji je podešen odmah nakon standardne instalacije OS-a), što ne ograničava ponuđača da koristi još novije verzije, pod uslovom da se radi o stabilnim verzijama i da ih sam pripremi za instalaciju, ili da koristi zadnju verziju, ili da pripremi izmjenjenu verziju (patch) konkretne softverske komponente.
I-13. Ponuđač može da, u cilju zadovoljenja određenih tehničkih zahtjeva, dodatno izvrši prilagođavanja na sistemu, izvrši instalaciju dodatnih softverskih komponenti, ili da izvrši nadogradnju/izmjenu softverskih komponenti (patch i sl.), razvije pomoćne programe (backup rutine i sl.), razvije softverske module u okviru postojećih softverskih komponenti ili razvije administratorske/korisničke interfejse (web i sl.), ili da razvije određenu funkcionalnost u cjelosti.
I-14. Ponuđač je dužan da kompletnu implementaciju svih ponuđenih rješenja, kao i tražena proširenja postojećih produkcionih sistema, izvrši u roku koji je dat u tenderskoj

dokumentaciji. FZOCG obezbjeđuje ispunjenost preduslova potrebnih za izvršenje aktivnosti u datom vremenskom roku, što uključuje: neometan pristup server sali i raspoloživost hardverskih, podataka i drugih resursa na lokaciji naručioca, opisanih u tenderskoj dokumentaciji.
I-15. Obzirom da je većina sistema u produkcionoj upotrebi gdje se toleriše veoma mali downtime ne duži od 10 min, neophodno je da ponuđač prilikom implementacije ponuđenih rješenja koristi prvo pasivni nod (backup nod) u okviru klaster grupa, a zatim da prebaci produkcioni sistem na pasivni nod, kako bi nastavio sa implementacijom na preostalim nodovima. Kod grupa koje imaju active/active nodove, potrebno je prvo proširiti sistem sa novim nodovima (koristiti predviđene pomoćne virtuelizovane i hardverske resurse, date specifikacijom iz tenderske dokumentacije), pa tek onda migrirati produkcioni sistem na tako novoimplementirane nodove kako bi se konačno oslobodili preostali nodovi za nastavak implementacije ponuđenih riješenja. Kod grupa koje imaju više od dva noda u klasteru, moguće je privremeno isključivanje do dva noda (na primjer odgovarajući par), kako bi se oslobodili postojeći produkcioni hardverski ili virtuelizovani resursi za novu implementaciju, a sve pod uslovom da u klaster grupi uvijek ostanu barem dva noda u produkciji. Za implementaciju pojedinačnih nodova, koji nisu sastavni dio klastera ili cijelina, ponuđač može privremeno koristiti predviđene pomoćne hardverske i virtuelizovane resurse, date specifikacijom iz tenderske dokumentacije, do završetka implementacije.  Sve aktivnosti je potrebno izvršiti uživo na sistemu.
2.2 Posebni zahtjevi i instrukcije za implementaciju ponuđenih rješenja
I-16. Ponuđena rješenja moraju da zadovoljavaju sve industrijske standarde predviđene tehničkim zahtjevima, kako bi integracija sa postojećim produkcionim okruženjem bila izvodljiva.
I-17. Platforma za virtuelizaciju se sastoji od KVM hipervizora, koji su redudantno povezeni na zajednički SDS storage sistem (10Gbps mreža), a međusobno i prema ostatku sistema su povezani preko

redudantnih veza na mrežne switcheve.
Moguće je isključiti do dva hipervizora istovremeno iz produkcionog klastera i to u strogo predviđenom vremenskom rasponu, a sve u cilju implementacije ponuđenog rješenja u ovom segmentu. Prije početka implementacije, sve virtuelne mašine sa hipervizora koji se privremeno isključuju će biti migrirane na preostale hipervizore a nakon implementacije ponuđenog rješenja, migrirane virtuelne mašine će biti vraćene na iste te hipervizore.
I-18. Za implementaciju ponuđenog rješenja u SSL gateway segmentu, FZOCG obezbijeđuje sve podatke potrebne za migraciju na ponuđeno rješenje (username, pin/tan liste, nazive institucija i korisnika, grupa privilegija, kao i međusobne relacije entiteta, x509 sertifikate).
I-19. Platforma VPN koncentratora se sastoji od dva virtuelizovana servera koja povezuju udaljene lokacije, koje se sastoje od jednog ili više računara (lica, ustanove, punktovi itd.). Određene lokacije preko zajedničkog Internet linka ostvaraju više paralelnih VPN konekcija
O-3. Ponuđač je dužan implementirati platformu za virtuelizaciju, uz zadovoljenje svih traženih tehničkih zahtjeva, u koracima od po dva noda u paru, na način da sve aktivnosti prvog nivoa podrške budu izvodljive preko svih serverskih nodova odmah nakon završetka sveukupne implementacije.
O-4. Vremenski raspon implementacije ponuđenog rješenja, u segmentu platforme za virtuelizaciju, za jedan par nodova ne može biti duži od 4h. Potrebno je izvršiti live backup (snapshot) svih virtuelnih mašina na svim hipervizorima, nakon završetka implementacije ponuđenog rješenja.
O-5. Ponuđač je dužan implementirati plaformu VPN koncentratora tako da je moguće konkurentno funkcionisanje većeg broja TCP konekcija sa računara udaljene lokacije koji su preko više paralelnih VPN konekcija povezani na sistem (preko zajedničkog Internet linka na udaljenoj lokaciji
2.3 Tehnička podrška
I-20. FZOCG obezbjeđuje prvi nivo podrške koji podrazumijeva svakodnevne operativne aktivnosti na sistemima koji su predmet

javne nabavke. Ponuđač obezbjeđuje drugi nivo tehničke podrške za sve komponente implementiranih sistema.
O-6. Ponuđač je dužan da ponudi drugi nivo tehničke podrške koji podrazumijeva operativne aktivnosti instalacije, konfiguracije, migracije, konsaltinga, preventivnog održavanja, otklanjanje tehničkih problema i izvršenje preporučenih upgrade-a komponenti sistema, kao i definisanje operativnih procedura za kvalitetno sprovođenje prvog nivoa podrške (na dnevnom, nedjeljnom i mjesečnom nivou).
P-1. Poželjno je da ponuđač u toku trajanja ugovora, a na zahtjev FZOCG, blagovremeno obezbijedi procedure i dokumentaciju koja sadrži procedure, detaljne opise, instalaciju, administraciju i korisničke priručnike za sve djelove sistema.
P-2. Ponuđači se pozivaju da dostave opise dodatnih funkcionalnosti sistema koje nijesu zahtijevane, a koje mogu služiti unapređenju sistema.
O-7. Neophodno je da ponuđač definiše procedure za prijavu problema kao i vremena odziva za sljedeće nivoe problema:
• Urgentni nivo problema
• Visok nivo problema
• Srednji nivo problema
• Nizak nivo problema.
I-21. Definicije nivoa problema su sledeće:
Urgentni nivo problema Sistem nije funkcionalan.
Visok nivo problema Problemi u dostupnosti servisa, ali većina korisnka može da dobije servis.
Srednji nivo problema Problemi koji trenutno ne ugrožavaju funkcionalnost servisa, ali mogu da utiču na funkcionalnost ukoliko se ne pristupi blagovremenom rješavanju
Nizak nivo problema Manji problemi ili tehnički zahtjevi koji ne utiču na funkcionalnost sistema

O-8. Za sve tipove problema ponuđač mora obezbjeđivati vrijeme privremenog i trajnog rješenja od momenta prijave problema, kao i raspoloživost resursa tehničke podrške za slučaj problema po principu 24/7/365.
Maksimalne vrijednosti vremena privremenog odnosno trajnog rješenja problema u odnosu na nivo problema su

date u tabeli:
Nivo problema Vrijeme privremenog rješenja Vrijeme trajnog rješenja
Urgentni 8h 36h
Visok 24h 1 nedjelja
Srednji 1 nedjelja 4 nedjelje
Nizak 3 nedjelje 6 nedjelja

O-9. Ponuđač je u obavezi da obezbjedi mogućnost prijave problema 24 sata dnevno i to na sljedeće načine: WEB portal za prijavu problema; e-mail; fax i telefon. U ponudi je neophodno navesti informacije za sve tražene načine prijave problema.
2.4 Sistemi i platforme
2.4.1 Firewall/Ruter
O-10. Firewall/ruter rješenje mora da podržava standardni set funkcionalnosti:
• Stateful i Stateless opciju filteringa paketa.
• 802.1q (vlan tagging)
• Troubleshooting alati (ping, traceroute, log)
• NAT (Network Address Translation)
• PAT (Port Address Translation)
• DHCP server (server za dodjelu dinamičkih IP adresa)
• Statičko rutiranje
• Backup/Restore konfiguracija,
• Kontrola udaljenog administratorskog pristupa, na način da pojedinačni privilegovani administratori, zaduženi za podešavanja Firewall/Ruter sistema, mogu pristupiti samo sa unaprijed određenih IP adresa.
O-11. Firewall/ruter rješenje mora da podržava napredni set funkcionalnosti:
• Združivanje mrežnih interfejsa (active/passive, agregacija)
• Rutiranje na osnovu polisa (tip saobraćaja, source i destination IP adrese, portovi)
• QoS (shaping i prioritetizacija na osnovu polisa ili odgovarajućih bitova u IP hederu paketa)
• OSPF dinamički ruting protokol, na način da omogućava sinhronizaciju jedne ili više ruting tabela operativnog Sistema
• Adaptivna performansna podešavanja za mrežnu brzinu/kašnjenje
• Adaptivni menadžment procesa i memorije u cilju efikasnog izvršavanja procesa u multiprocesorskom okruženju sa više sistemskih magistrala
• Automatsko balansiranje procesorskih prekida između jezgara u realnom vremenu

u skladu sa uslovima rada sistema.
• Aplikativni balanser saobraćaja po HTTP protokolu: prema različitim unutrašnjim putanjama i uz ravnomjernu distribuciju saobraćaja; zadržavanje saobraćaja sesije prema istoj unutrašnjoj putanji do završetka sesije; praćenje ispravnosti unutrašnjih putanja i preusmjeravanje saobraćaja prema ispravnim putanjama u slučaju ispada.
O-12. Firewall/ruter rješenje mora da podržava visoko-dostupne (High Availiability - HA) konfiguracije (active/passive).
O-13. Firewall/ruter rješenje treba da omogućava administratorski interfejs/alat, ili konfiguracione fajlove, na način da podržava izvršenje tipičnih dnevnih aktivnost prvog nivoa podrške.
I-22. Tipični poslovi obavljanja prvog nivoa podrške kod ovog sistema podrazumijeva definisanje i mijenjanje sljedećih parametara: interfejsa, firewall pravila, mrežnih ruta, NAT; zatim, backup/restore aktivnosti i analizu logova.
I-23. Firewall sistem je u produkcionom okruženju implementiran u modu active/backup na dva servera prema specifikaciji hardverskih resursa iz tenderske dokumentacije.
2.4.2 VPN Koncentrator
O-14. VPN koncentrator rješenje mora da podržava opciju za terminaciju IPSEC tunela.
O-15. VPN koncentrator rješenje mora da podržava AES, SHA i Diffie Hellman Grupe podešavanja za IKE i ESP enkripcione transformacije, minimum: aes128, aes192, aes256, sha1,sha256,sha384,dh-2,5,14,15.
O-16. VPN koncentrator rješenje mora da podržava pojedinačno ili kombinaciju opcija, PSK, x509, i password identifikaciju udaljenih lokacija, koje su ukačene po IPSEC protokolu. Podržane kombinacije navedenih opcija, ili podešavanje pojedinačnih opcija, moraju da podržavaju kačenje sledećih klijenata: Cisco VPN klijent, Linux klijenti, Apple iPhone klijent, Windows 7 i Windows 10 klijent, Juniper klijent.
O-17. VPN koncentrator rješenje mora da podržava opciju za NAT-T (nat traversal) protokol.
O-18. VPN koncentrator rješenje mora da podržava opciju za DPD (dead peer detection) protokol.

O-19. VPN koncentrator rješenje mora da podržava opciju za IP kompresiju tuneliranih paketa.
O-20. VPN koncentrator rješenje mora da podržava dinamički protokol za razmjenu ključeva IKEv1 i IKEv2.
O-21. VPN koncentrator rješenje mora da podržava automatsko spuštanje mrežnih ruta po IKEv1 i IKEv2 protokolu, za svaku klijentsku VPN konekciju pojedinačno.
O-22. VPN koncentrator rješenje mora da podržava uspostavljanje PPTP tunela prema udaljenim lokacijama (MSCHAPv2, MPPE). Samo se jedan server u klaster grupi koristi za ovu namjenu, na način što se unaprijed odredi od strane FZOCG.
O-23. VPN koncentrator rješenje mora da podržava PKI (Public Key Infrastructure) elemente koji su potrebni za ažuriranje x.509 sertifikata – (CA, generate, revoke, crl liste, crl URL, OCSP provjeru).
O-24. VPN koncentrator mora da podržava konfiguraciju access lista po IPSEC konekciji.
O-25. VPN koncentrator rješenje mora da podržava osnovni i napredni set firewall/ruter funkcionalnosti iz tehničkih zahtjeva.
O-26. VPN koncentrator rješenje mora da podržava rad u u grupi od više koncentratora, na način da u slučaju ispada jednog koncentratora, sve raskinute udaljene konekcije mogu da se preraspodjele na preostale koncentratore u grupi, odnosno svi koncentratori unutar grupe moraju da imaju ulogu aktivnih nodova prema kojima se automatski uspostavljaju VPN konekcije udaljenih lokacija.
O-27. VPN koncentrator riješenje mora da pruža NTP servis ostatku mreže FZOCG, na način da se sinhronizuje sa barem 4 udaljena NTP referentna izvora, kao i da su svi koncentratori referentno sinhronizovani između sebe.
O-28. VPN koncentrator rješenje treba da omogućava administratorski interfejs/alat, ili konfiguracione fajlove, na način da podržava izvršenje tipičnih dnevnih aktivnost prvog nivoa podrške.
I-24. Tipični poslovi obavljanja prvog nivoa podrške kod ovog sistema podrazumijeva definisanje i mijenjanje sljedećih parametara: korisnika, x509 sertifikata, interfejsa, firewall pravila, ruta, NAT; zatim, backup/restore

aktivnosti i analizu logova.
I-25. VPN koncentrator sistem je u trenutnom produkcionom okruženju implementiran u modu active/active (svi serveri imaju ulogu aktivnih nodova), na dvije virtuelizovane mašine prema specifikaciji virtuelizovanih resursa iz tenderske dokumentacije.
2.4.3 SSL gateway
O-29. SSL gateway rješenje mora da podržava terminaciju SSL/TLS zaštićenih konekcija preko HTTP protokola (HTTPS tip konekcije) za udaljene lokacije (IP adresa udaljenih lokacija nisu unaprijed poznate).
O-30. SSL gateway rješenje mora da podržava konfiguraciju zasebnog x509 sertifikata za svaki domen/profil HTTPS konekcije pojedinačno.
O-31. SSL gateway rješenje mora da podržava identifikaciju HTTPS konekcija po modelu korisničkog naloga i pin koda.
O-32. SSL gateway rješenje treba da podržava naprednu identifikaciju HTTPS konekcija, za sveukupan saobraćaj po tim konekcijama, po modelu PIN/TAN sistema (bankarski standard za authentifikaciju baziran na jednokratnim kodovima za autentifikaciju).
O-33. SSL gateway rješenje mora da podržava konfiguraciju unutrašnje URL putanje na koju se preusmjeravaju dolazni zahtjevi, za svaki profil spoljašnje HTTPS konekcije pojedinačno, na način da omogućava privilegije pristupa prema unutrašnjim URL putanjama po grupama identifikovanih korisnika (privilegije na nivou grupa).
O-34. SSL gateway mora da omogućava WEB administratorski i korisnički interfejs, na način da se prikaz interfejsa automatski prilagođava veličini ekrana na uređaju sa kojeg se pokreće interfejs (mobile-responsive karakteristika).
O-35. SSL gateway rješenje treba da omogućava administratorski interfejs na način da podržava izvršenje tipičnih dnevnih aktivnost prvog nivoa podrške.
O-36. SSL gateway rješenje treba da omogućava korisnički interfejs na način da podržava korisnički pristup unutrašnjim URL putanjama na osnovu date grupe privilegija i to nakon uspješne autentifikacije sa korisničkim nalogom, pinom i jednokratnom

lozinkom sa TAN lista, zatim, da omogućava interfejs za promjenu PIN-a, generisanje novih TAN lista, kao i vizuelni indikator da je lista sa TAN kodovoima pri kraju (uskoro istrošena).
O-37. SSL gateway mora da podržava visoko-dostupne (High Availiability - HA) i skalabilne konfiguracije, na način da ravnomjerno distribuira zahtjeva prema aplikativnim instancama. U slučaju ispada nekog od nodova toleriše se ponovno uspostavljanje konekcija i identifikacija korisnika.
I-26. Tipični poslovi obavljanja prvog nivoa podrške kod ovog sistema podrazumijeva definisanje i ažuriranje sljedećih parametara: ustanova, korisnika, grupa privilegija, PIN/TAN lista, unutrašnjih URL putanja).
I-27. FZOCG obezbijeđuje važeći potpisani x509 sertifikat, do 5 domena, koji se sastoji od javnog i privatnog ključa, kao i javnog ključa CA koja je izdala sertifikat, a sve u standardnom elektronskom formatu.
I-28. Za implementaciju SSL gateway rješenja,u skladu sa datim tehničkim zahtjevima, su previđene virtuelizovane mašine prema specifikaciji virtuelizovanih resursa iz tenderske dokumentacije.
2.4.4 Virtuelizacija servera
O-38. Platforma za virtuelizaciju servera mora da podržava virtuelizaciju gost mašina (virtuelne mašine), baziranu na KVM tehnologiji, i to bez izmjena na nivou gost mašine, uz podržane hipervizor servere x86_64 procesorske arhitekture (cpu namjene za virtuelizaciju).
O-39. Platforma za virtuelizaciju servera mora da podržava Linux OS (32bit i 64bit) gost virtuelne mašine.
O-40. Platforma za virtuelizaciju servera mora da podržava sledeće Microsoft Windows  gost virtuelne mašine: Windows Server 2012, Windows 2003 server, Windows 2008 server, Windows XP, Windows 7. Platforma za virtuelizaciju mora da podržava rješenje za migraciju (OS i podaci) fizički odvojenih računara (sa CD/DVD uređajemi mrežnom karticom) u gost virtuelne mašine (sa kompatibilnom konfiguracijom – broj procesora, količina radne memorije, veličina diska, magistrale, grafička kartica itd.) za sledeće Microsoft Windows operativne sisteme: Windows XP,

Windows 7 i Windows 2003 server.
O-41. Platforma za virtuelizaciju servera mora da podržava kreiranje novih virtuelnih mašina po unaprijed definisanom template-u (broj procesora i diskova, veličina diska i ram memorije, preinstalirani operativni sistem).
O-42. Platforma za virtuelizaciju servera mora da podržava tehniku pozajmljivanja memorija između virtuelnih mašina (memory-ballooning) u slučaju kompatibilnog OS-a na gost virtuelnoj mašini.
O-43. Platforma za virtuelizaciju servera mora da podržava kreiranje backupa od diska virtuelne mašina bez obaranje same virtuelne mašine (shutdown), odnosno neosjetno za rad virtuelne mašine (live-snapshot funkcionalnost).
O-44. Platforma za virtuelizaciju servera mora da podržava NAS/NFS, Fiber channel i iSCSI topologije veza prema storage sistemu, kao i da podržava integraciju preko interfejsa za smještanje blokova podataka (block disk) na SDS sistem na kojem će se nalaziti glavni raspoloživi kapaciteti sa skladištenje podataka.
O-45. Platforma za virtuelizaciju mora da podržava klasterizovani fajl sistem OCFSv2.
O-46. Platforma za virtuelizaciju mora da podržava podešavanje I/O virtuelizacije mrežnih interfejsa i direktnu dodjelu virtuelizovanog mrežnog segmenta mašinama tako da je moguća live migracija između odgovarajućeg para hipervizora.
O-47. Platforma za virtuelizaciju servera treba da omogućava administratorski interfejs/alat, ili konfiguracione fajlove, na način da podržava izvršenje tipičnih dnevnih aktivnost prvog nivoa podrške.
I-29. Tipični poslovi obavljanja prvog nivoa podrške kod ovog sistema podrazumijeva kreiranje virtuelnih mašina i njihovo podešavanje, migracija virtuelnih mašina između hipervizora “uživo” (live migration), kreiranje i dodjela mrežnih interfejsa, “uživo” backup virtuelnih mašina (live snapshot), migracija Win7/XP/2003server fizičkih mašina u gost virtuelne mašine, automatizovana migracija svih virtuelnih mašina sa jednog hipervizora na drugi.
I-30. Platforma za virtuelizaciju se u produkcionom okruženju sastoji od šest hipervizora (prema specifikaciji hardverskih resursa iz tenderske dokumentacije),

povezana na zajednički SDS storage sistem, redudantnim 10Gbps, koja omogućavaju uživo migraciju mašina između hipervizora, uživo backup (snapshot) diska virtuelnih mašina, kao i konverziju između storage image formata prema potrebi.  Za namjenu podrške migraciji fizičkih Windows računara u gost virtuelne mašine je predviđen odvojeni server (prema specifikaciji hardverskih resursa iz tenderske dokumentacije).
2.4.5 Mail sistem
O-48. Mail sistem rješenje treba da podržava standardne protokole mail komunikacije uz obaveznu enkripciju preko istih ili odvojenih portova: POP3, SMTP, IMAP.
O-49. Mail sistem rješenje treba da podržava SUBMISSION port za slanje mailova, na način da je obavezna prethodna autentifikacija korisnika prije slanja/transfera maila prema serveru. Slanje mailova preko standardnog SMTP porta, od strane korisnika FZOCG, nije dozvoljeno, već se standardni SMTP port koristi samo za primanje mailova za lokalne domene.
O-50. Mail sistem rješenje mora da podržava SPF i DKIM mehanizme prema DMARC preporuci, kao i da obezbijeđuje ARC implementaciju. Mail sistem rješenje mora da podržava PFS mehanizam.
O-51. Mail sistem rješenje treba da podržava Webmail interfejs. Webmail interfejs mora da podržava opcije za auto-responder, email filtere i personalizovane potpise, pregled i konstruisanje HTML email poruka.
O-52. Mail server rješenje mora da podržava deduplikaciju i kompresiju mejl sadržaja na način da se minimizuje skladišteni prostor tako da isti mejl sadržaj poslat/primljen na više adresa bude uskladišten tačno jednom. Mail server rješenje mora da podržava brzu pretragu (ispod 1s) za mejl sanduče koje broji velike količine mejlova (50.000 mejlova i više).
O-53. Mail server rješenje treba da podržava Anti-Spam i Anti-Virus mehanizme zaštite po korisničkom nalogu za dolazni i odlazni saobraćaj. Mail server rješenje mora da podržava definisanje proizvoljne anti-spam politike određivanja da li je mejl sadržaj spam.
O-54. Mail server rješenje treba da podržava konfigurisanje (uključivanje/isključivanje)

pojedinačnih servisa po korisničkom nalogu i to za sledeće pojedinačne privilegije/pristupe: SMTP, POP3, IMAP, Anti-Spam i Anti-Virus, podešavanje filtera i preusmjeravanje maila.
O-55. Mail server rješenje mora da podržava korisničke klase servisa za ograničenja i propusne kontrole u jedinici vremena (minuti) za odlazni saobraćaj u predefinisanim periodima i danima u toku nedjelje, a sve mjereno pojedinačno po korisničkom nalogu/adresi, uz mogućnost definisanja proizvoljnih smtp-greška poruka: maksimalni broj mejlova u jedinici vremena, maksimalni broj primalaca u jedinici vremena, maksimalnu ukupnu veličinu mejlova u jedinici vremena, maksimalnu veličinu pojedinačnog mejla.
O-56. Mail server rješenje mora da podržava prijemne klase servisa za ograničenja i propusne kontrole u jedinici vremena (minuti) za dolazni saobraćaj u predefinisanim periodima i danima u toku nedjelje, uz mogućnost definisanja proizvoljnih smtp-greška poruka: maksimalni broj konekcija u jedinici vremena, maksimalni broj pokušaja isporuke u jedinici vremena na osnovu broja aktivnih RBL listinga (predefinisane liste), maksimalni broj pokušaja isporuke na osnovu regexp pretrage po hostname/helo parametrima SMTP konekcije.
O-57. Mail server rješenje mora da podržava blokiranje isporuke mejla na osnovu otiska SSL sertifikata udaljenog servera koji pokušava isporučiti poštu.
O-58. Mail server rješenje mora da podržava definisanje proizvoljnog perioda i privremene smtp-greške koju će sistem javljati za zakazana održavanja sistema, u okviru kojeg privremeno neće biti dozvoljeno primanje ili slanje mejlova.
O-59. Mail server rješenje mora da podržava automatsko serversko dodavanje sadržaja na kraju odlaznog mejla (prema destinacijama van sistema). Sadržaj se definiše u HTML i TXT formatu po korisniku, a odgovarajuća varijanta se dodaje u zavisnosti od tipa mejla (HTML i/ili TXT).
O-60. Mail server rješenje mora da obezbjeđuje konfiguraciju u skladu sa vodećim preporukama, tako da zadovoljava sve testove i propratne preporuke na online Internet testu MXToolBox. Online adresa

preko koje se testira je:
https://mxtoolbox.com.
O-61. Mail sistem rješenje treba da omogućava administratorski interfejs/alat, ili konfiguracione fajlove,  na način da podržava izvršenje tipičnih dnevnih aktivnost prvog nivoa podrške.
I-31. Tipični poslovi obavljanja prvog nivoa podrške kod ovog sistema podrazumijeva kreiranje, brisanje korisničkih naloga, upravljanje mejl aliasima, promjena lozinke, backup mailova po korisničkom nalogu, kao i analiza logova.
I-32. Za implementaciju mail sistema je predviđena jedna virtuelna mašina, prema specifikaciji virtuelizovanih resursa iz tenderske dokumentacije.

2.4.6 Sistem za mrežni monitoring
O-62. Sistem za mrežni monitoring mora da podržava praćenje dostupnosti servisa po TCP, UDP i ICMP (ping) mrežnim protokolima.
O-63. Sistem za mrežni monitoring mora da podržava mehanizme za praćenje dostupnosti servisa (na primjer: http, mail i sl.).
O-64. Sistem za mrežni monitoring mora da podržava mehanizme za prikupljanje informacija po SNMP protokolu, koristeći mehanizam “SNMP trap” i prikupljanje SYSLOG logova, te generisanje događaja na osnovu prikupljenih informacija. Obavezna je implementacija slanja SNMP trap poruka u slučaju ispada agregacija mrežnih interfejsa na serverskim nodovima koji imaju podešenu mrežnu redudantnost.
O-65. Sistem za mrežni monitoring mora da podržava ručno ubacivanje nodova za praćenje, kao i automatsko traženje dostupnih nodova na osnovu zadate mreže, i automatsko traženje dostupnih servisa na pronađenom nodu.
O-66. Sistem za mrežni monitoring mora da podržava slanje email poruka u sastavnom dijelu notifikacionih mehanizama.
O-67. Sistem za mrežni monitoring mora da podržava generisanje i prikazivanje grafika praćenih podataka (na primjer: in/out bytes i sl.).
O-68. Sistem za mrežni monitoring treba da omogućava administratorski interfejs/alat, ili konfiguracione fajlove,  na način da

podržava izvršenje tipičnih dnevnih aktivnost prvog nivoa podrške.
I-33. Tipični poslovi obavljanja prvog nivoa podrške kod ovog sistema podrazumijeva administraciju pravila za praćenje, pregled podataka i relevantnih izvještaja stanja.
I-34. FZOCG će samostalno izvršiti unos pravila za praćenje u sistemu za mrežni monitoring, nakon sveobuhvatne implementacije svih ostalih sistema.
I-35. Za implementaciju sistema za mrežni monitoring je predviđena jedna virtuelna mašina, prema specifikaciji virtuelizovanih resursa iz tenderske dokumentacije.
2.4.7 Proxy sistem
O-69. Proxy sistem mora da podržava keširanje web saobraćaja (HTTP).
O-70. Proxy sistem mora da podržava filtriranje web zahtjeva po tipu sadržaja (exe, zip, doc, excel i slične formate).
O-71. Proxy sistem mora da podržava filtriranje web saobraćaja po ključnim riječima.
O-72. Proxy sistem mora da podržava filtriranje web zahtjeva po URL adresama.
O-73. Proxy sistem mora da podržava konfiguraciju prava pristupa po jednoj ili više korisničkih IP adresa, po danima u nedjelji.
O-74. Proxy sistem mora da podržava mehanizme za integraciju sa trećim sistemima za analizu/adaptaciju sadržaja (na primjer: u cilju antivirus skeniranje, ubacivanje upozorenja o sumnjivom sadržaju i sl. ).
O-75. Proxy sistem mora da podržava transparentno presretanje i filtriranje enkriptovanog web saobraćaja (https).
O-76. Proxy sistem mora da omogućava administratorski interfejs/alat, ili konfiguracione fajlove, na način da podržava izvršenje tipičnih dnevnih aktivnost prvog nivoa podrške.
I-36. Tipične dnevne aktivnosti na ovom sistemu podrazumijevaju konfiguraciju različitih podržanih filtera i polisa.
I-37. Za implementaciju Proxy sistema je prdviđena jedna virtuelna mašina, prema specifikaciji virtuelizovanih resursa iz tenderske dokumentacije.
2.4.8 DNS sistem
O-77. DNS sistem mora da podržava konfiguracije autoritativnog, slave, forvardera ili kešing dns sistema.

O-78. DNS sistem mora da minimalno podržava sledeće resurs rekorda u okviru konfiguracije zona:
• A (address record)
• NS (name server record)
• PTR (pointer record)
• CNAME (canonical name record)
• TXT (text record)
• SPF (sender policy framework record)
• MX (mail exchange record)
• SRV (service locator).
O-79. DNS sistem mora da podržava AXFR mehanizam za transfer zona.
O-80. DNS sistem mora da podržava Split-Horizon funkcionalnost.
O-81. DNS sistem treba da omogućava administratorski interfejs/alat, ili konfiguracione fajlove, na način da podržava izvršenje tipičnih dnevnih aktivnost prvog nivoa podrške.
I-38. Tipične dnevne aktivnosti na ovom sistemu podrazumijevaju konfiguraciju različitih tipova resurs rekorda.
I-39. Za implementaciju DNS sistema u produkcionom okruženju je predviđena jedna virtuelna mašina prema specifikaciji virtuelizovanih resursa iz tenderske dokumentacije, kao i jedna udaljena serverska instanca na Internetu za slave implementaciju.
2.4.9 SSO sistem
I-40. Zbog većeg broja servera kojima administratori FZOCG pristupaju svakodnevno, zatim, unapređenja kontrole pristupa i sigurnosti svekupnog sistema, kao i potrebe jednostavnog prenosa fajlova između servera odvojenih mrežnih segmenata, potrebno je implemenitrati SSO sistem sa zaštićenim mrežnim direktorijumom.
O-82. Ponuđač mora da implementira riješenje za SSO sistem, koje omogućava administratorski pristup serverima sa radnih stanica, po modelu identifikacije preko korisničkog naloga/passworda unošenjem passworda samo jednom (SSO / single-sign-on), nakon čega se administratoru odobrava pristup (preko SSH ili drugog mehanizma) bez ponovne autentifikacije passwordom, i sve to direktno sa radne stanice administratora.
O-83. SSO sistem mora da omogući administratoru način da se odjavi, sa čime

mu se uklanjaju prethodno date privilegije pristupa bez ponovnog unošenja passworda.
O-84. Mogućnost pristupa serverima na standardan način preko username/passworda mora ostati nepromjenjena, za slučaj da administrator ne želi da koristi u datom momentu SSO sistem.
O-85. Kada administrator pristupi serveru, potrebno je da mu se automatski poveže personalizovani mrežni direktorijum na tom serveru sa centralne lokacije, za koji samo on ima prava pristupa (drugi ulogovani administratori ne mogu da pristupe tom direktorijumu za slučaj da se nalaze na istom serveru). Ukoliko se administrator uloguje na više servera istovremeno, mrežni direktorijum mora biti dostupan na svim serverima, zadržavajući prava pristupa samo tom adminstratoru.
O-86. Transfer fajlova između servera kojem se pristupa i mrežnog direktorijuma mora biti enkriptovan sa odgovarajućim algoritmom, koji mora biti industrijski standard. Navesti algoritam koji će se koristiti za enkripciju u ponuđenom riješenju.
I-41. Za implementaciju svih navedenih tehničkih zahtjeva SSO sistema su predviđene virtuelne mašine, prema specifikaciji virtuelizovanih resursa iz tenderske dokumentacije.
2.4.10 VPN klijent
O-87. Ponuđač mora da obezbijedi VPN klijent rješenje, koje je podržano na Linux distribucijama koje se trenutno koriste u FZOCG (zadnja verzija Ubuntu LTS, CentOS i RockyLinux distribucije), tako da podržava automatsko uspostavljanje IPSec konekcija (podržana oba protokola IKEv1 i IKEv2) prema VPN koncentratorima FZOCG, sa podržanim automatskim prihvatanjem mrežnih ruta od strane VPN koncentratora, kao i provjeru validnosti serverskog sertifikata po CRL i/ili OCSP putanji koja je upisana u sertifikatu.
O-88. VPN klijent rješenje treba da omogućava administratorski interfejs/alat, ili konfiguracione fajlove, na način da podržava izvršenje tipičnih dnevnih aktivnost prvog nivoa podrške.
O-89. Potrebno je da ponuđač obezbijedi odgovarajuću podršku za dijagnostiku prilikom problema u uspostavljanju IPSEC

konekcija sa Linux i Microsoft Windows operativnih sistema, kao i sa drugih podržanih uređaja.
I-42. Tipične dnevne aktivnosti na VPN klijentskom sistemu podrazumijevaju: konfiguraciju IPSEC klijentskih tunela.
I-43. VPN klijentsko riješenje se u produkcionom okruženju instalira od strane administratora FZOCG prema procedurama koje definiše ponuđač, odnosno nije obaveza ponuđača da izvršava konkretnu instalaciju VPN klijenta, već samo da obezbijedi VPN klijentsko riješenje prema tehničkom zahtjevu.
2.4.11 SMS gateway
O-90. SMS Gateway mora da podržava integraciju sa SMS centrom mobilnih operatora po protokolu SMPP verzija 3.3 i 3.4.
O-91. SMS Gateway mora da podržava udruživanje više paralelnih konekcija prema istom SMS centru mobilnog operatora i ravnomjerno balansiranje slanja SMS poruka preko tako udruženih konekcija.
O-92. SMS Gateway mora da podržava podešavanje različitih profila konekcija prema SMS centrima mobilnih operatora sa mogućnošću podešavanje parametara SMPP protokola (profili za različite mobilne operatore sa različitim varijantama SMPP podešavanja).
O-93. SMS Gateway mora da podržava integraciju korisničkih servisa preko REST web servisa: za slanje poruka, primanje poruka preko kratkog koda, kao i za dobijanje povratnih notifikacija o uspješnosti isporuke.
O-94. SMS Gateway mora da podržava mehanizam autentifikacije REST web servisa preko dodijeljenog sigurnosnog tokena (token se prenosi kao “query” parametar u HTTP zahtjevu web servisa).
O-95. SMS Gateway mora da podržava podešavanje više korisničkih profila u okviru kojih se definišu parametri servisa: sigurnosni token za REST web servis, dozvoljeni filteri telefonskih brojeva, dozvoljeni SMS centri za upotrebu, maksimalno vrijeme života poruke (ttl), predefinisani templejt REST adrese za slanje povratnih notifikacija.
O-96. SMS Gateway mora da podržava podešavanje REST templejta adrese koja će

se prozivati za svaku dobijenu notifikaciju o uspješnosti isporuke SMS poruke – u slučaju da je podešena.
O-97. SMS Gateway mora da podržava upisivanje, u fajlove i u bazu podataka, zapisa o svakoj poslatoj poruci prema SMS centrima mobilnog operatera sa svim pratećim parametrima koji jednoznačno određuju korišćeni servis (accounting zapisi): vrijeme, SMS centar, servisni i/ili korisnički profil, sadržaj poruke, primaoce i pošiljaoce, notifikacione informacije.
O-98. SMS Gateway mora da podržava telekomunikacioni “back-off” protokol za odloženo slanje SMS poruka u slučaju trenutne nemogućnosti SMS centra mobilnog operatora da primi poruku za dalje slanje. “back-off” protokol predviđa da svaki naredni pokušaj slanja poruke se odlaže za dodatno vrijeme, kako bi se izbjegla eventualna zagušenja, a nakon predviđenog broja iteracija dolazi do trajnog prekida procesa.
O-99. SMS Gateway mora da podržava privremeno čuvanje u trajnom storage prostoru (hard disk) svih prihvaćenih a neisporučenih SMS poruka i notifikacija, za oba pravca, ka SMS centru ili ka korisničkim servisima, sve do konačne isporuke – “Queue” sa predefinisanim vremenom trajanja pokušaja za poruke koje ne mogu biti trenutno obrađene.
O-100. SMS Gateway mora da podržava ograničavanje brzine protoka SMS poruka (broj poruka u sekundi) za svaku konekciju prema SMS centru mobilnog operatora pojedinačno, kao i logovanje trenutnog protoka u sistemskom logu u cilju formiranja istorije iskorišćenosti kapaciteta.
O-101. SMS Gateway mora da podržava slanje i primanje poruka sa ASCII i UNICODE formatom zapisa sadržaja SMS poruke, kao i opciju tekstualnog formata pošiljaoca.
O-102. SMS Gateway mora da podržava podešavanje kratkih kodova i preusmjeravanje dolazećih SMS poruka pema korisničkim servisima na osnovu prve riječi iz sadržaja SMS poruke, kao i da omogućava mehanizam da se odgovori na tako prispjele poruke vrate prema krajnjem korisniku preko istog SMS centra mobilnog operatora sa kojeg su došle.

O-103. SMS Gateway mora da podržava grupno slanje SMS poruka na način da se isti sadržaj poruke pošalje na sve brojeve iz tekstualnog fajla. Grupno slanje poruka se aktivira ručno od strane administratora sistema.
O-104. SMS gateway mora da omogući konfigurisanje univerzalne HTTP URL adrese za slanje poruka u formatu: http://[adresa servera]:[port]/1.0/sendsms/[brojTelefona]. [brojTelefona] – broj telefona na koji se šalje sa prefikom +382. “Query” http parametri su: [text] – sadržaj sms poruke, [token] – sigurnosni token iz korisničkog profila.
I-44. Tipične aktivnosti prvog nivoa podrške za SMS gateway su: podešavanje korisničkih profila, konekcija prema mobilnim operatorima, pregled accounting zapisa.
I-45. Za implementaciju svih navedenih tehničkih zahtjeva SMS gateway-a su predviđene virtuelne mašine, prema specifikaciji virtuelizovanih resursa iz tenderske dokumentacije.
2.4.12 Crypto sistem
I-46. Naručilac obezbjeđuje HSM modul na kojem su smješteni privatno/javni ključevi osnovnih sertifikacionih tijela sa x509 sertifikatima i AES-256 domenski ključ. Za komunikaciju sa HSM modulom se koristi PKCS11 interfejs. Parametri za povezivanje na HSM modul su: drajver, slot, PIN, identifikacione labele objekata (privatno/javni ključ, x509 sertifikat, AES ključ). Takođe, naručilac definiše dodatne AES-GCM autentifikacione parametre u skladu sa upotrebom. Svi parametri će biti dostupni u momentu konfigurisanja sistema. Sve strukture za skladištenje i razmjenu binarnih informacija (enkriptovanih ili binarno formatiranih) moraju biti otvorenog tipa tj. učitavanje podataka mora biti uvijek moguće nezavisno od ponuđenog rješenja - prateći opisane mehanizme, protokole i standarde.
O-105. Sistem mora da podržava kriptografske funkcije za generisanje AES-256 ključeva i enkripciju/dekripciju podataka po AES-GCM algoritamu (vektor dužina 96 bita, uporedna tag dužina 128 bita) uz dodatne autentifikacione parametre - naznačeni algoritam. Naznačeni algoritam mora uvijek da se koristi u procesima gdje se

predviđa enkripcija/dekripcija informacija (ukoliko drugačije nije traženo), a krajnji rezultat enkripcije (enkriptovani fajlovi, enkriptovani odgovori od webservisa, enkriptovani podaci, enkriptovani ključevi i sl.) mora da bude strukturno formatiran tako da se prvo upiše korišćeni vektor inicijalizacije, odmah u nastavku da slijedi enkriptovani sadržaj, tek na kraju da se upiše tag, dok enkriptovan sadržaj može da ima i svoju strukturu organizacije podataka tj. format.
O-106. Sistem mora da omogućava hijerarhiju AES ključeva, kao i mjesto poziva kriptografskih operacija (na HSM modulu ili van modula), na način: I nivo - domenski i posrednički ključ, II nivo - klijentski ključevi i III nivo - omotni ključevi; Domenski ključ i kriptografske operacije na HSM modulu se koriste za kreiranje/enkripciju/dekripciju posredničkog ključa. Posrednički ključ se koristi za enkripciju/dekripciju klijentskih ključeva i pratećih informacija u vezi sa servisom gdje se koriste klijentski ključevi. Klijentski ključevi se koriste za enkripciju/dekripciju podataka i za enkripciju/dekripciju omotnih ključeva. U radu sa klijentskim i omotnim ključevima se koriste kriptografske operacije isključivo van HSM modula (nije potrebno prisustvo HSM modula).
O-107. Sistem mora da podržava generisanje AES-256 posredničkog ključa. Posrednički ključ mora da se skladišti u jednom fajlu na disku, gdje fajl mora biti enkriptovan koristeći domenski ključ sa HSM modula i zasebno podešene dodatne autentifikacione parametre, sve po naznačenom algoritmu. Posrednički ključ se učitava isključivo prilikom starta sistema uz prisustvo HSM modula i ostaje učitan sve do narednog (re)starta sistema.
O-108. Sistem mora da podržava generisanje AES-256 klijentskih ključeva i da podržava mehanizam rotacije klijentskog ključa. Entitet klijentskog ključa mora da sadrži osnovne podatke (Meta) i inkrementalne verzije sirovog AES-256 ključa (Verzije). Meta podatak mora da uključuje: jedinstveni identifikator (na primjer: c3c0600a-e0aa-4a47-8882-e09a1134ed00) po UUIDv4 (ID), datum kreiranja po RFC3339 (Datum), deskriptivni opis (Opis) i

indikator trenutne validnosti ključa (Validan). Verzija ključa mora da sadrži broj koji se uvećava (Inkrement) i sirovi AES-256 ključ (Kljuc). Mehanizam rotacije podrazumjeva generisanje novog AES-256 sirovog ključa uz povećanje inkrementa verzije za 1. Aktuelna verzija ključa je ona sa najvećim inkrementom. Klijentski ključ mora da se skladišti u jednom fajlu na disku, sa binarnim zapisom po 'Protocol Buffers' (proto3) mehanizmu za serijalizaciju struktuiranih podataka, sa sljedećom definicijom zapisa "message KlijentskiKljuc{MetaPodatak Meta=1;repeated Verzija Verzije=2;} message MetaPodatak{string ID=1;string Datum=2;string Opis=3;bool Validan=4;} message Verzija{int64 Inkrement=1;bytes Kljuc=2;}", gdje fajl mora biti enkriptovan koristeći posrednički ključ i podešene dodatne autentifikacione parametre, sve po naznačenom algoritmu.
O-109. Sistem mora da omogućava webservis pozive za enkripciju/dekripciju podataka pomoću klijentskog ključa. Za proces enkripcije, sistem mora da uvijek koristi aktuelnu verziju klijentskog ključa. Argumenti poziva webservisa za enkripciju podataka uključuju  podatak koji treba enkriptovati, identifikator klijentskog ključa i dodatni autentifikacioni parametar, a odgovor uključuje enkriptovani sadržaj. Enkriptovani sadržaj se sastoji od dvije enkriptovane informacije i mora biti formatiran strukturno tako da sadrži prvo enkriptovan pokazivač korišćenog klijentskog ključa, a u nastavku da se nalazi enkriptovani podatak. Pokazivač  klijentskog ključa se enkriptuje sa posredničkim ključem i formatiran je strukturno na način da prvo sadrži jedinstveni identifikator klijentskog ključa, zatim, separator karakter '#', i na kraju uvijek petocifrenu verziju ključa (nule se dodaju na početak verzije kao dopuna do pet cifara). Argumenti poziva webservisa za dekripciju podataka uključuju enkriptovani sadržaj (nastao ranije u procesu enkripcije) i dodatni autentifikacioni parametar, a odgovor uključuje  dekriptovani podatak.
O-110. Sistem mora da omogućava webservis poziv za ponovnu enkripciju već enkriptovanog podatka sa drugim ključem (zamjena klijentskog ključa). Argumenti poziva webservisa uključuju enkriptovani

sadržaj, identifikator novog klijentskog ključa i dodatni autentifikacioni parametar, a odgovor uključuje novoenkriptovani sadržaj.
O-111. Sistem mora da omogućava webservis za generisanje AES-256 omotnog ključa. Argumenti poziva webservisa uključuju identifikator klijentskog ključa i dodatni autentifikacioni parametar, a odgovor webservisa uključuje sirovi omotni ključ i enkriptovani sadržaj sa omotnim ključem. Za dekripciju sadržaja sa omotnim ključem se koristi specificirani webservis za dekripciju podataka. (Omotna kriptografija podrazumjeva enkripciju/dekripciju podataka koja se izvršava na strani klijenta, a sistem se koristi samo za generisanje jednokratnih (ne skladište se na strani sistema) omotnih ključeva. Sirovi omotni ključ se uništava po okončanju procesa enkripcije/dekripcije podatka na strani klijenta.)
O-112. Sistem mora da podržava automatsko rotiranje klijentskih ključeva na godišnjem nivou, tako da se u naznačenom intervalu generiše novi AES ključ (nova verzija klijentskog ključa) koji važi od tog momenta, ali tako da je moguće sprovesti dekripciju podataka koji su enkriptovani sa nekom od prethodnih verzija klijentskog ključa, a sve u skladu sa formatom entiteta klijentskog ključa.
O-113. Rješenje mora da omogućava CLI alat, na ponuđenoj Linux distribuciji, koji obavlja enkripciju/dekripciju fajlova po AES-CTR algoritmu ('all-zero' vektor inicijalizacije) koristeći zasebno generisani omotni ključ za svaki fajl pojedinačno, sa neophodnim okvirom komandnih argumenata i koristeći samo potrebne webservise za omotnu kriptografiju. Enkriptovani sadržaj sa omotnim ključem, kao i sami enkriptovani fajl, moraju da se smještaju u zasebnim fajlovima sa predefinisanim nazivom - tako što se na naziv originalnog fajla dodaje sufiks ".key" ili ".encrypted" u zavisnosti da li se radi, redom, o enkriptovanom ključu ili enkriptovanom fajlu.
O-114. Rješenje mora da omogućava CLI alat, na ponuđenoj Linux distribuciji, koji obavlja 'offline' dekripciju fajlova (na nezavisnim serverskim mašinama van mreže) po AES-CTR algoritmu ('all-zero' vektor inicijalizacije) koristeći omotni ključ, sa neophodnim okvirom komandnih

argumenata, gdje je lokalno na serverskoj mašini dostupan samo HSM modul, posrednički ključ, odgovarajući klijentski ključ, enkriptovani omotni ključ i enkriptovani fajl. (Parametri za rad sa HSM modulom i dodatni autenfikacioni parametri se zadaju u momentu korišćenja CLI alata.)
O-115. Sistem mora da podržava import fajlova koji sadrže ključeve (posrednički i klijentski ključevi) na način da je dovoljno samo kopirati fajlove u odgovarajući direktorijum i opcionalno restartovati sistem, nakon čega odmah mora da bude moguća njihova upotreba.
O-116. Sistem mora da podržava rad sa više osnovnih sertifikacionih tijela (RootCA) sa HSM modula (u skladu sa odgovarajućim pristupnim parametrima), kao i upravljanje kriptografskim operacijama sa HSM modula u procesima generisanja i potpisivanja sertifikata.
O-117. Sistem mora da podržava kreiranje više posredničkih sertifikacionih tijela (Intermediate CA), tako što će posrednički CA sertifikati biti potpisani od strane odabranog osnovnog sertifikacionog tijela sa HSM modula, a privatni ključ od posredničkog sertifikacionog tijela mora biti smješten na disku u enkriptovanom fajlu po naznačenom enkripcionom algoritmu (koristeći pridruženi klijentski ključ od nadležnog posredničkog CA).
O-118. Sistem mora da podržava generisanje x509 sertifikata sa 2048 i 4096-bitnim RSA ključevima i ECDSA ključevima sa krivim P-224, P-256, P-384 i P-521. Privatni ključevi se u sistemu mogu skladištiti isključivo enkriptovano po naznačenom enkripcionom algoritmu koristeći pridruženi klijentski ključ od nadležnog posredničkog CA.
O-119. Sistem mora da podržava potpisivanje sertifikata sa posredničkim sertifikacionim tijelom (posrednički CA), gdje su sertifikati generisani unutar sistema, kao i potpisivanje po zahtjevu za potpisivanje sertifikata (CSR zahtjev) i da podržava digitalne potpise SHA-128, SHA-256, SHA-384, SHA-512.
O-120. Sistem mora da podržava eksport potpisanog sertifikata (prethodno generisan u sistemu), odgovarajućeg privatnog ključa, kao i CA lanca (osnovni+posrednički), sve

zajedno u p12 formatu. Sistem mora da omogućava eksport bilo kojeg pojedinačnog sertifikata u PEM formatu.
O-121. Sistem mora da podržava podešavanje više PKI (Public Key Infrastructure) profila sa proizvoljnim elementima koji su potrebni za ažuriranje x.509 sertifikata (kombinacija ekstenzija za posebne namjene x.509 sertifikata).
O-122. Sistem mora da podržava OCSP serverske tačke (endpoint) u cilju provjere validnosti sertifikata od strane udaljenih klijenata, kao i da se predviđene OCSP putanje upisuju u sertifikat.
O-123. Sistem mora da omogućava upravljačko rješenje zasnovano na web tehnologijama tako da je na klijentskoj strani dovoljno koristiti samo web browser u cilju rada sa grafičkim korisničkim interfejsom, sve tako da podržava izvršenje tipičnih dnevnih aktivnost prvog nivoa podrške. Upravljačko riješenje mora imati razdvojenu komponentu baze podataka sa omogućenim zasebnim pristupom za DB administratora.
O-124. Upravljačko rješenje mora da podržava softverski modul za svu neophodnu administraciju sistema. (na primjer: unos korisnika, podešavanja prava i privilegija i sl.).
O-125. Upravljačko rješenje mora da podržava multikorisničko okruženje gdje se za pristup sistemu koristi autorizacija sa korisničkim nalogom i lozinkom.
O-126. Upravljačko rješenje mora da podržava sistem prava i privilegija koje se preko konfigurabilnih rola dodijelju korisnicima sistema. Prava i privilegije generički moraju da obuhvataju podešavanje definicija za pristup softverskim modulima (cjeline administracija i kriptografija), određenim stranicama unutar modula (generisanje klijentskih ključeva, sertifikata i sl.), ključnim entitetima (korisnik, sertifikat, klijentski ključ i sl.), atributima entiteta (datum generisanja, ime, prezime, opis i sl.) i specifične privilegije. Specifične privilegije obuhvataju: pravo za generisanje posredničkih sertifikacionih tijela, pravo za potpisivanje sertifikata, pravo za eksport sertifikata, pravo za generisanje klijentskih AES ključeva, pravo pristupa REST web servisima, pravo pristupa grafičkom korisničkom interfejsu, pravo pristupa

korisničkom interfejsu interaktivne dokumentacije web servisa.
O-127. Upravljačko rješenje mora da podržava definisanje proizvoljnih logičkih kombinacija uslova filtera za pretragu ključnih entiteta iz modela.
O-128. Upravljačko rješenje mora da podržava eksport podataka u Excel formatu uz svaku tabelu koja prikazuje atribute entita iz modela, pri čemu korisnik može sam da označi kolone, redosled kolona i redove koji će biti eksportovani. Za označavanje redova, korisnik može da koristi kombinacije logičkih uslova filtera pretrage, i to sve kroz više korisničkih iteracija zadavanja upita pretrage dok ne formira željenu selekciju podataka za eksport.
O-129. Upravljačko rješenje mora da podržava upis svih vremenskih podataka u bazi podataka sa vremenskom zonom UTC i da potrebne mehanizme rada sa vremenskim zona realizuju unutar aplikacije, tako da promjena vremenske zone na samom operativnom sistemu servera nije od uticaja na već upisane vremenske podatke u bazi podataka.
O-130. Upravljačko rješenje mora da podržava praćenje i trajno čuvanje svih izmjena nad entitetima modela i pripadajućim relacijama, kao i praćenje obrisanih podataka, u svrhu sigurnosnog traga (“audit trail”). Svaki zapis praćenja mora jasno da ukazuje na atribute entiteta koji su izmjenjeni, uz podatke o vremenu, koji korisnik je izvršio izmjenu, i porijeklu izmjene (grafički korisnički interfejs ili REST web servis). Svaki od entiteta pojedinačno mora da sadrži podatke o vremenu i korisniku koji je prvi put kreirao entitet modela, kao i zadnji put izmijenio entitet modela. Pristup ovim informacijama mora biti omogućen nezavisno od korisničkog interfejsa aplikacije.
O-131. Upravljačko rješenje mora da podržava integraciju sa trećim sistemima preko REST web servisa. Za pristup REST web servisima od strane trećih sistema se koristi mehanizam autorizacije preko korisničkog naloga i lozinke, koji se ujedno mogu koristiti i za pristup grafičkom korisničkom interfejsu. Za korisnike web servisa iz trećih sistema, a nakon uspješne autentifikacije, se prvo registruje sesija tako

da za sve naredne pozive web servise nije potrebna ponovna autentifikacije već se uz poziv proslijeđuje samo indikator sesije.
O-132. Upravljačko rješenje mora da podržava prepoznavanje indikatora korisničke sesije iz predefinisanog nezavisnog atributa iz zaglavlja (hedera) i iz “Cookie”-a  HTTP zahtjeva. Klijentska strana može ravnopravno da koristi ili jedan ili drugi mehanizam smještanja indikatora korisničke sesije u HTTP zahtjevu.
O-133. Upravljačko rješenje mora da podržava interaktivnu dokumentaciju REST web servisa, gdje se opis poziva nalazi kao dio integrisan u okviru grafičkog korisničkog interfejsa (sastavni dio administratorskog modula aplikacije) zajedno sa mogućnošću poziva uživo - preko forme u okviru koje se popunjavaju parametri poziva tog web servisa.
O-134. Upravljačko rješenje mora da podržava administratorske opcije za odjavu svih korisnika (logout all), slanje poruka svim korisnicima (broadcast), pregled svih aktivnih korisničkih sesija grafičkog korisničkog interfejsa i web servisa. Pregled mora da uključuje vrijeme zadnje aktivnosti korisnika. Broadcast poruke se prikazuju u svim browser prozorima ulogovanog korisnika i blokiraju korisnički interfejs sve dok korisnik ne zatvori poruku. Opcija za odjavu svih korisnika se izvršava odmah bez ikakvog korisničkog upozorenja, ali tako da ne izloguje administratora koji je pokrenuo odjavu svih korisnika.
O-135. Upravljačko rješenje mora da podržava višejezičko okruženje grafičkog korisničkog interfejsa, tako da obezbjeđuje mogućnost podešavanje jezika za pojedinačnog korisnika kroz administratorski interfejs. Upravljačko rješenje mora da obezbjeđuje opciju za Crnogorski (default) i Engleski jezik.
O-136. Upravljačko rješenje mora da podržava istorijske zapise svih korisničkih sesija, koje moraju imati sledeće atribute entiteta: jedinstveni identifikator sesije, IP adresa, vrijeme početka i kraja sesije, tip sesije (grafički korisnički interfejs ili web servis sesija), korisnik, i opisne informacije klijentskog web browsera.
O-137. Softversko rješenje mora da podržava automatski dnevni backup svih

podataka i odlaganje u trajnu arhivu na udaljenom serveru preko SCP ili FTP protokola.

O-138. Upravljačko rješenje mora da podržava klasterizovanu implementaciju. Implementacija mora da obezbijeđuje: dostupnost svih relevantnih komponenti u slučaju ispada nekog od nodova u klasteru; skalabilnost čitanja iz baze podataka; skalabilnost aplikativne logike sa dodavanjem novih odgovarajućih komponenti u klaster; raspoređivanje novih korisničkih sesija u odnosu na 5-minutno prosječno zauzeće procesora da bi se postiglo adekvatno iskorišćenje predviđenih kapaciteta. U slučaju ispada, toleriše se gubitak uspostavljenih sesija samo sa nedostupnog noda.
O-139. Ponuđač mora da obezbijedi razvojnu podršku u periodu do 30 dana za eventualne dodatne manje izmjene i prilagođavanja na sistemu kako bi Naručilac bolje upodobio sistem prema svojim potrebama.
I-47. Tipične aktivnosti prvog nivoa podrške za sistem su: generisanje, pretraga, poništavanje i eksport sertifikata (korisničkih sertifikata i posredničkih CA tijela), ažuriranje baze poništenih sertifikata, generisanje AES ključeva, podrška u radu sa web servisima, enkripcija/dekripcija fajlova na strain drugih sistema.
I-48. Za implementaciju svih navedenih tehničkih zahtjeva Crypto sistema su predviđene virtuelne mašine, na način da su serverski razdvojene ključne logičke funkcionalnosti (upravljački interfejs / aplikacija, HSM kriptografske operacije, verifikacija certifikata / OCSP tačka), prema specifikaciji virtuelizovanih resursa iz tenderske dokumentacije.
2.4.13 Trustpoint sistem
O-140. Trustpoint  rješenje mora da podržava terminaciju SSL/TLS enkriptovanih konekcija preko HTTP 1.1 i 2.0 protokola (https konekcije), kao i WebSocket-a sa udaljenih lokacija (preko http-upgrade mehanizma), i njihovo preusmjeravanje prema unutrašnjim servisnim URL putanjama (po principu balansiranja).
O-141. Trustpoint  rješenje mora da podržava podešavanje HTTPS endpoint-a sa

unutrašnjim servisnim URL putanjama uz mogućnost definisanja zasebnog x509 sertifikata po endpoint-u i autentifikaciju udaljenih lokacija sa zasebnim CA sertifikatom.
O-142. Trustpoint rješenje mora da podržava osnovnu autentifikaciju udaljenih lokacija po modelu korisničkog naloga i lozinke po http protokolu.
O-143. Trustpoint rješenje mora da podržava preusmjeravanja dolaznog endpoint saobraćaja prema unutrašnjim URL putanjama u skladu sa predefinisanim algoritmom: round-robin, least connection i hashing po parametrima iz HTTP zahtjeva. Algorimi za balansiranje moraju da podržavaju opciju za ‘sticky’ sesije (na osnovu cookie-a) tako da aktivna sesija završava uvijek na istu unutrašnju URL putanju gdje je i prvi put uspostavljena.
O-144. Trustpoint rješenje mora da podržava fail-over između unutrašnjih URL putanja, gdje u slučaju ispada, dolazana konekcija se preusmjerava prema narednoj ispravnoj lokaciji u skladu sa algoritmom za balansiranje.
O-145. Trustpoint rješenje mora da podržava provjere ispravnosti (health check) unutrašnjih URL putanja u predefinisanim vremenskim intervalima po HTTP protokolu, na proizvoljnoj URL putanji i portu, za svaku unutrašnju putanju pojedinačno, na način da provjera statusni kod odgovora sa strane konkretnog servisa uz odgovarajuće maksimalno vrijeme čekanja (timeout).
O-146. Trustpoint rješenje mora da u slučaju pojave učestanih neispravnosti unutrašnjih servisa u predviđenom vremenskom intervalu isključi problematičnu unutrašnju putanju na određeno vrijeme, bez obzira što ona za neke zahtjeve prethodno ponekad vraća ispravne odgovore. (mogućnost dodatnog vremena za eventualnu stabilizaciju servisa).
O-147. Trustpoint rješenje mora da podržava visoko-dostupne (High Availiability - HA) implementacije. U slučaju ispada nekog od nodova u klasteru, toleriše se ponovno uspostavljanje konekcija i identifikacija udaljenih lokacija.
O-148. Trustpoint rješenje mora da podržava servisne http pristupne liste (access list) za svaku od unutrašnjih putanja pojedinačno,

po svim tipovima http zahtjeva (GET, POST, DELETE itd.) i unutrašnjoj URL putanji.
O-149. Trustpoint rješenje mora da obezbjeđuje konfiguraciju SSL/TLS protokolnih parametara u skladu sa vodećim sigurnosnim preporukama, tako da na online Internet testu (Qualys SSL Labs - SSL Server test) ne smije da dobije manju ocijenu od “A”. Online adresa preko koje se testira je: https://www.ssllabs.com/ssltest/
O-150. Trustpoint rješenje mora da podržava osnovni i napredni set firewall/ruter mrežnih funkcionalnosti iz tehničkih zahtjeva.
O-151. Trustpoint rješenje treba da omogućava administratorski interfejs/alat, ili konfiguracione fajlove, na način da podržava izvršenje tipičnih dnevnih aktivnost prvog nivoa podrške.
I-49. Tipične aktivnosti prvog nivoa podrške za ovaj sistem su: podešavanje unutrašnjih putanja i endpoint-a, ažuriranje mrežnih ruta, pregled logova, podešavanje x509 i drugih sigurnosnih parametara.
I-50. Za implementaciju svih navedenih tehničkih zahtjeva Trustpoint sistema su predviđene virtuelne mašine, prema specifikaciji virtuelizovanih resursa iz tenderske dokumentacije.
2.4.14 SDS sistem (Software-Defined-Storage)
O-152. SDS sistem mora da omogućava visoko-skalabilno klasterizovano skladište za smještanje fajlova, objekata i blokova podataka (block disk) na način da sastavni softverski slojevi omogućavaju nezavisnost od posebno specijalizovanog hardvera.
O-153. SDS sistem mora da omogućava pozadinsko ravnomjerno distrubuiranje podataka unutar klastera, kontinuiranu pozadinsku provjeru integriteta podataka i samostalni oporavak u slučaju ispada.
O-154. SDS sistem mora da omogućava nadogradnju softvera u fazama bez ili sa minimalnim vremenom prekida rada klastera.
O-155. SDS sistem mora da podržava protokole AWS S3 i Swift za rad sa objektima, integracione mehanizme sa KVM hipervizorima za virtuelizaciju diska od virtuelnih mašina, integraciju sa standardnim Linux-zasnovanim fizičkim serverima za rad sa blokovima podataka (pridruženim diskom) preko mreže i POSIX-kompatibilni

klasterizovani fajl sistem (dijeljiv pristup ka fajl sistemu između više klijenata).
O-156. SDS sistem mora da omogućava grafički interfejs za monitoring i dijagnostiku sistema, uključujući statistiku korišćenja za čitav klaster i pojedinačno po komponentama.
O-157. SDS sistem mora da omogućava kontrolu pristupa za korisnike sistema po nivoima smještenih podatka (na primjer: ‘pools’, ‘object buckets’, putanje ka fajlovima i sl).
O-158. SDS sistem mora da omogućava enkripciju objekata na osnovu proslijeđenih kriptografskih ključeva u zahtjevu bez ikakve specijalne konfiguracije na sistemu da bi se podržao ovaj enkripcioni režim.
O-159. SDS sistem mora da omogući adekvatnu algoritamsku zaštitu dugoročnosti podataka uz podržanu visoku dostupnost podatka i visoke performanse pri radu sa podacima, a sve uz odgovarajuću ekonomičnost u pogledu smještajnih kapaciteta.
O-160. SDS sistem mora da omogućava proširenje ili smanjenje blokova podataka bez prekida u radu sistema (downtime).
O-161. SDS sistem mora da omogućava podešavanja polisa za smještanje podataka u skladu sa performansnim zahtjevima, odgovarajućom skladištenom lokacijom (na primjer: sporiji ili brži diskovi za smještanje podataka) i domenima mogućih ispada (na primjer: rack ormar, ili spratnost data centra).
O-162. SDS sistem mora da omogućava momentalne snimke blokova podataka (snapshots) bez prekida u radu sistema ili značajnih penala po performanse i odziv sistema u datom momentu.
O-163. SDS sistem mora da omogućava distribuciju klijentskih konekcija za prenos podataka preko cijelog klastera na način da ne postoji pojedinačna tačka mogućeg ispada u komunikaciji (single point of failure).
O-164. SDS sistem mora da omogućava kloniranje blokova podataka na način da se od jednog bloka podataka može momentalno izdvojiti brojne kopije nezavisnih blokova podataka, bez prekida u radu sistema ili značajnih penala po performanse i odziv sistema u datom momentu.
O-165. SDS sistem mora da omogućava

implementaciju finog podešavanja za veće performanse pri upisivanju podataka kroz odgovarajuće žurnaling/kešing tehnologije.
O-166. SDS sistem mora da podržava replikaciju objekata između lokacija i automatsko arhiviranje verzija objekata.
O-167. SDS sistem mora da omogućava dimenzioniranje blokova podataka na način da ukupna veličina tek kreirianog bloka može da prelazi veličinu instalisanih kapaciteta (thin provisioning).
O-168. SDS sistem mora da omogućava replikaciju blokova podataka na udaljenu DR (disaster recovery) lokaciju. SDS sistem mora da omogućava automatizovani mehanizam za backup objekata po BACKUP-3-2-1 pravilu – najmanje tri kopije podataka, barem dva različita medijuma za smještanje, gdje jedna kopija mora biti van glavne lokacije.
O-169. BACKUP-3-2-1 sistem mora da uključuje implementaciju primarnog SDS sistema, sa kojeg se prenose podaci prema backup SDS sistemu, sa kojeg se preuzimaju podaci inicirano sa backup servera povezanog na biblioteku traka. Za vezu između backup servera i SDS sistema za prenos podataka potrebno je implementirati HPS (high-performance switching) gateway na SDS sisteme (standardni mrežni saobraćaj se sa jedne strane rutira prema uređajima za visoko-performantni switching unutar SDS sistema).
U okviru BACKUP-3-2-1 sistema moraju biti implementirani procesi za izradu rezervnih kopija podataka i automatizovanu rotaciju traka (automatizovano snimanje nastavlja na narednu traku sve do iskorišćenja zadnje trake, kada sistem nastavlja ponovo da snima počev od prve trake) i to procesi: automatizovano za sve logičke rezervne kopije sa predviđenih lokacija skladišta objekata na dnevnom nivou na zasebnom rotacionom pool-u traka; za sve rezervne kopije slika blokova podataka (na zahtjev) na zasebnom rotacionom pool-u traka; za izradu šifriranih rezervnih kopija (na zahtjev) na trake koje se odlažu van zgrade. Na kraju svakog pokrenutog procesa za izradu rezervnih kopija na trake potrebno je na backup serveru čuvati do dvije godine sve izvještaje, kao i slati te izvještaje na predefinisane mejl adrese. Izvještaji moraju

minimalno da uključuju identifikator rezervne kopije, nazive datoteka ili druge reference koje su ušle u datu rezervnu kopiju, serijski broj trake, redni broj arhive na traci i prostorno zauzeće napravljene rezervne kopije na traci. Pravo/privilegije za pokretanje procesa za izradu rezervnih kopija na sistemu mora biti dodijeljeno samo određenim korisnicima na način da ti korisnici ne mogu ništa drugo da izvrše na sistemu (isključuvo pokretanje procesa za izradu rezervnih kopija, bez mogućnosti izvršavanja bilo koje druge komande na sistemu). Nakon implementacije je potrebno dostaviti dokumentovane procedure za izradu i oporavak podataka sa traka na osnovu implementiranih procesa u skladu sa datim opisima, kao i proceduru za generisanje novog ključa za šifrovanje podataka.
O-170. SDS rješenje treba da omogućava administratorski interfejs/alat, ili konfiguracione fajlove, na način da podržava izvršenje svih administratorskih aktivnosti.
I-51. Za implementaciju svih navedenih tehničkih zahtjeva SDS sistema su predviđene fizičke mašine, prema specifikaciji hardverskih resursa iz tenderske dokumentacije. Za sistem backupa podataka su predviđeni resursi za implementaciju zasebnog backup SDS sistema (pored produkcionog SDS sistema), kao i nezavisni backup server na izdvojenoj lokaciji van glavne lokacije (BACKUP 3-2-1 pravilo), biblioteka za trake i server za implementaciju HPS gateway-a.
3. SPECIFIKACIJA PRODUKCIONOG I POMOĆNOG HARDVERA I VIRTUELIZOVANIH RESURSA
3.1. Hardver i virtuelizovani resursi predviđeni za produkciono okruženje

Hardver sa sledećom specifikacijom:
- Firewall/Ruter
HP DL360G10, Intel (R) Xeon Gold (R) CPU 6144 3,5 GHz, 2 CPU, 8 cores, 2x300 GB HDD, 32 GB RAM, 1Gb Ethernet 4-port Adapter, 10Gb/40Gb 2-port +QSFP Adapter, 2 napajanja.
HP DL360G10, Intel(R) Xeon(R) Silver 4114 CPU @ 2.20GHz, 2 CPU, 10 cores, 2x300 GB HDD, 32 GB RAM, 1Gb Ethernet 4-port

Adapter, 10Gb/40Gb 2-port +QSFP Adapter, 2 napajanja;
- Platforma za virtuelizaciju
Hipervizori :
(povezani na SDS sistem)
7 x (HP DL360G10, Intel (R) Xeon (R) Gold CPU 5122 3.6 GHz, 2 CPU,  4 cores, 2 threads per core, 2x900 GB SAS, 256 GB RAM, 4x10Gbps NIC, 1Gb Ethernet 4-port Adapter, 2 napajanja)
Podrška migraciji fizičkih računara u gost virtuelne mašine :
1x DL360G10 ,Intel (R) Xeon Gold (R) CPU 5122 3.6 GHz, 2 CPU,  2x600GB HDD, 64GB RAM, 4x10Gbps NIC, 4x1Gbps NIC.
- SDS sistem
11x DL360G10 ,Intel (R) Xeon Gold (R) CPU 6248 2.5 GHz, 2 CPU,  2x600GB HDD, 192GB RAM, 2x10Gbps NIC, 2x40Gbps NIC, 4x1Gbps NIC , 4x3.5TB SSD, 1x750GB NVMe SSD
3x DL360G10 ,Intel (R) Xeon Silver (R) CPU 4208 2.1 GHz, 2 CPU,  2x600GB HDD, 64GB RAM, 2x10Gbps NIC, 4x1Gbps NIC
1x DL360G10 ,Intel (R) Xeon Gold (R) CPU 5122 3.6 GHz, 2 CPU,  2x600GB HDD, 64GB RAM, 4x10Gbps NIC, 4x1Gbps NIC
- Backup SDS
5 x (HP DL380G10, Intel (R) Xeon (R) Gold CPU 5122 3.6 GHz, 2 CPU,  4 cores, 2 x 240GB SATA RI M.2 SSD, 10 x 10TB SAS 7.2K LFF SC He 512e DS HDD,  GB RAM, 4x10Gbps NIC, 1Gb Ethernet 4-port Adapter, 2 napajanja)
- Backup Server
1 x (HP DL380G10, Intel (R) Xeon (R) Gold 2.5 GHz, 2 CPU,  10 cores, 7 x 16 TB SATA, 1 x 512 GB SSD , 2 x 128 GB NVMe drives, 128 GB RAM, 7 x HDD 16TB SATA 7.2K LFF SC He 512e DS HDD, 1 x Ethernet 10 GB SFP, 1Gb Ethernet 4-port  Adapter, 2 napajanja)

1x TAPE LIBRARY
- Tejp lajbreri uredjaj (uredjaj biblioteke traka) namjenjen za montazu u rek orman, podrska za 48 tejp drajv uredjaja i 640 slotova za trake samostalno ili putem dodatnih modula za nadogradnju Sistema
- tri (3) ugradjena uredjaja traka ("tejp drajv") LTO-9 Ultrium 45000 sa SAS interfejsom
- četrdeset (40) ukljucenih slotova za trake

- HPS  gateway (High-performance switching)
1x (HP DL360G10, Intel (R) Xeon (R) Gold CPU 5122 3.6 GHz, 2 CPU,  4 cores, 2 threads per core, 2x900 GB SAS, 256 GB RAM, 4x10Gbps NIC, 1Gb Ethernet 4-port Adapter, 2 napajanja), povezan sa optičkim kablom direktno na backup server

- TESTNI SERVER
DL360G10 ,Intel (R) Xeon Gold (R) CPU 5122 3.6 GHz, 2 CPU,  2x600GB HDD, 64GB RAM, 4x10Gbps NIC, 4x1Gbps NIC
Virtuelizovani resursi sa sledećom specifikacijom:
- DNS sistem
1 virtuelna mašina: 1 CPU, 1GB RAM, 8GB HDD, 1 NIC.
1 instanca na Internetu (slave): 1 CPU, 1GB RAM, 8GB HDD, 1 NIC, 1x javna IP adresa.
- Proxy sistem
1 virtuelna mašina :1 CPU, 1GB RAM, 10GB HDD, 2 NIC
- VPN platforma
2 virtuelne mašine (4 CPU, 4 GB RAM, 12GB HDD, 2 NIC)
- SSO sistem (Single Sign-on platforma)
do 2 virtuelne mašine  (zbirno: 4 CPU, 4GB RAM, 40GB HDD, 3+ NIC)
- Sistem za mrežni monitoring
1 virtuelna mašina (2 CPU, 4 GB RAM, 30GB HDD, 1+ NIC)
- SSL gateway
1 virtuelna mašina (2 CPU, 4GB RAM, 20GB HDD, 2 NIC)
- SMS gateway
1 virtuelna mašina :1 CPU, 1GB RAM, 20GB HDD, 1 NIC
- Crypto sistem
1 virtuelna mašina: 4 CPU, 8GB RAM, 30GB HDD, 1 NIC
1 virtuelna mašina: 2 CPU, 2GB RAM, 30GB HDD, 1 NIC
1 virtuelna mašina: 2 CPU, 2GB RAM, 30GB HDD, 1 NIC
- Trustpoint sistem
1 virtuelna mašina  (4 CPU, 8 GB RAM, 20GB HDD, 3 NIC)
- Mail sistem
1 virtuelna mašina  (4 CPU, 16 GB RAM, 30GB HDD, 1TB HDD, 2 NIC)

| | | | | | |
|---|---|---|---|---|---|
| | | | 4.2 Predviđeni privremeni hardverski resursi i virtuelne mašine<br>Predviđeni su privremeni hardverski resursi i virtuelne mašine, dostupne do završetka implementacije:<br>- VM serveri za ostalu privremenu upotrebu<br>6 x virtuelna mašina: 2 CPU, 2GB RAM, 8GB HDD, 2+ NIC. | | |

***Izvještaj generisan 16.10.2024 10:31***