

Tehniline kirjeldus

Kaskaadteavituse infosüsteemi kasutuslitsentsi soetamine

1. Hanke eesmärk ja üldsätted

- 1.1. Kaskaadteavituse infosüsteemi (edaspidi ka **alarmeerimistarkvara või tarkvara**) soetamine.
- 1.2. Tehniline kirjeldus on aluseks hankelepingutele, mis sõlmitakse raamlepingu alusel kasutuslitsentside soetamiseks (kasutuslitsents, erisused toodud ptk 8).

2. Nõuded alarmeerimistarkvara funktsionaalsusele

2.1. Teadete saatmine peab olema võimalik järgmiste kanalite kaudu:

- 2.1.1. Krüptitult nutiseadme apliksiooni kaudu (Android ja iOS operatsioonisüsteemides);
- 2.1.2. SMS-i kaudu;
- 2.1.3. E-maili kaudu;
- 2.1.4. Audiokõne kaudu;
- 2.1.5. Läbi eelsalvestatud automaatkõnede.

2.2. Tarkvara liidestatus:

- 2.2.1. Active Directory süsteemidega (kasutajakontode ajakohaseks haldamiseks);
- 2.2.2. Valmisolek liidestamiseks haiglate ja kiirabipidajate infosüsteemidega, kasutades integratsiooni protokolle ja mustreid, sealhulgas: SOAP, XML, HL7, BizTalk, REST, JSON.

2.3. Tarkvara peab võimaldama:

- 2.3.1. Edastada haiglate ja kiirabipidajate osakondadel igapäevaseid väljakutseid puuduva personali asendamiseks;
- 2.3.2. Teavitada personali kriisisituatsiooni väljakutse vajadusest;
- 2.3.3. Saada personalilt kiiret tagasisidet väljakutsele vastamise (OK/NOK) koos eeldatava saabumisaajaga¹;
- 2.3.4. Analüüsida alarmeerimise järgselt saadud tagasiside põhjal osakondade mehitatuse taset ja vajadusi;
- 2.3.5. Üheaegselt alarmeerida vajadusel kogu asutuse personali operatiivselt erinevatest ohuolukordadest;
- 2.3.6. Jagada operatiivselt käitumisjuhiseid vastavalt ohuolukorrale ja/või selle tasemele;
- 2.3.7. Luua erinevaid kasutajagruppe ja adressaadigruppe vastavalt oskustele, erialale, sündmuse tüübile, osakondade kaupa jne;
- 2.3.8. Luua ühiskontosid tavakasutaja, dispetšeri ja administraatori rollile;
- 2.3.9. Luua ja saata eelkoostatud sõnumeid ning teavitusi.

2.4. Teadete edastamise omadused:

- 2.4.1. Tarkvara peab võimaldama valida sõnumiedastuse viisi (kas üks või mitmed korraga);

¹ Tarkvara on kahesuunaline kommunikatsioonikanal, mis tähendab, et läbi tarkvara saadetakse personalile teade, millele saab teate saaja omakorda vastata (nõustuda või keelduda) ning teate saatja näeb, kuidas personal on vastanud.

- 2.4.2. Tarkvara peab võimaldama edastada teate vähemalt 8000 lõppkasutajale maksimaalselt 10 minuti jooksul;
- 2.4.3. Tarkvara peab võimaldama teate adressaadil teatele analüüsitavas vormis vastata;
- 2.4.4. Tarkvara peab võimaldama lõppkasutaja vastuste reaajas jälgitavust ning analüüsi;
- 2.4.5. Juhul, kui on valitud mitmed teate edastamise viisid, toimub sõnumite saatmine eelseadistatud järjestuses (näiteks esmalt läbi nutiseadme aplikatsiooni, seejärel lühisõnumitega ning seejärel audiokõne/e-mailiga);
- 2.4.6. Kui teatega otsitakse ühte vastajat, siis esimene „OK“ vastanu saab valitud, temale väljastatakse automaatselt sellekohane teade ning teistele algse teate saajatele väljastatakse automaatselt teade, et positsioon on täidetud, rohkem inimesi ei otsita;
 - 2.4.6.1. Lisaks on teate saatjal võimalik ise kinnitada otsitavate töötajate sobivuse, kellele väljastatakse automaatselt sellekohane teade ning teistele algse teate saajatele väljastatakse automaatselt teade, et positsioonid on täidetud;
- 2.4.7. Tarkvara peab võimaldama määrata sõnumile prioriteetsuse aste ja sellest lähtuvalt alarmeerimise (näiteks esimese prioriteediga teade eirab telefoni personaalseid vaikesätteid);
- 2.4.8. Tarkvara peab võimaldama luua sõnumimalle ja saata eelkoostatud sõnumeid;
- 2.4.9. Tarkvara peab võimaldama lisada sõnumile faile (nt .jpg);
- 2.4.10. Tarkvara peab võimaldama aplikatsiooni kaudu kontaktidega suhtlemist live-sõnumite vahetamise teel.

2.5. Kasutajagrupid ja -funktsioonid:

- 2.5.1. Tarkvara peab võimaldama luua piiramatult erinevaid kasutaja- ja adressaadigruppe (vastavalt oskustele, erialale, sündmuse tüübile, osakondade kaupa jmt);
- 2.5.2. Tarkvara peab võimaldama saada ülevaadet, kui palju kasutajaid on *online* ja *offline*.

2.6. Logid:

- 2.6.1. Tarkvara peab võimaldama administraator-kasutajatel vaadata logisid (postkast), milles on kirjeldatud:
 - 2.6.1.1. Saadetud teate sisu;
 - 2.6.1.2. Kes on vastanud OK;
 - 2.6.1.3. Kes on vastanud NOK;
 - 2.6.1.4. Kes on saatnud lisainfot sõnumile vastates;
 - 2.6.1.5. Kes ei ole üldse vastanud;
 - 2.6.1.6. Kellele teade kohale ei jõudnud.

2.7. Majutus:

- 2.7.1. Täitja vastutab tarkvara majutamise eest kogu raamlepingu perioodil. Majutusega seotud kulud kannab täitja ning selle maksumus peab sisalduma teenuse hinnas.

3. Nõuded alarmeerimistarkvara tehnilisele toele ja hooldusele:

- 3.1. Pakkuja tagab *online* tehnilise toe ja hoolduse (ka **tootetugi**) tööpäevadel 08:00-16:00, v.a kriitiliste probleemide korral, mil tugi peab olema kättesaadav

ööpäevaringselt. Tootetoena mõistavad pooled eelkõige tõrgete ja probleemide kõrvaldamist tarkvaras, kas pakkuja algatusel või tellija teavituse alusel, versiooniuuenduste võimaldamist jmt tarkvara kasutamise parendustegevusi, mis on vajalikud tarkvara tõrgeteta toimimise tagamiseks.

3.2. Pakkuja tagab teenushäirete kõrvaldamise kiiruseks:

3.2.1. Kriitilistel² pöördumistel on reageerimise aeg kuni 4 tundi, probleemi kõrvaldamise või lahendamise aeg kuni 1 tööpäev;

3.2.2. Ülejäänud pöördumistel on reageerimise aeg kuni 2 tööpäeva ning probleemi kõrvaldamise või lahendamise aeg kuni 5 tööpäeva.

3.3. Tarkvaral on pakkuja poolne automaatne 24/7 monitooring pakkumuses esitatud infokanali kaudu.

4. Nõuded alarmeerimistarkvara logide pidamisele ja andmete varundamisele:

4.1. Logid:

4.1.1. Kõik infosüsteemi muudatused/tegevused (sh kasutajakontode, dokumentide, taotluste jms olekud), rakenduse ja kasutajate tegevused logitakse seostatult konkreetse füüsilise isikuga ja tema rolliga (nt juriidiline isik koos õigusega), kes muudatuse/tegevuse teostas;

4.1.2. Logikirje tekitamisel peab olema lisatud logikirje sõnaline selgitus, kui ei ole tegemist töötlemata veaolukorraga;

4.1.3. Tarkvara peab andmebaasi tasemel koguma audit-logi andmemuudatustest. Audit-logi peab sisaldama lisaks algandmetele ka tegevuse aega, tegevuse läbiviijat ning tegevuse tunnust (lisamine, muutmine, kustutamine). Audit-logi ei tohi saada muuta, st õiguslikult on lubatud vaid sündmuste lisamine ja pärimine;

4.1.4. Audit- ja tegevuslogisid säilitatakse 6 kuud pärast nende tekkimist, pärast mida logid kustutatakse.

4.2. Varundamine:

4.2.1. Nii andmekogus sisalduvad kui ka muud esmatähtsad andmed varundatakse regulaarselt, et oleksid tagatud seadustest ning tööprotsessidest tulenevad käideldavuse ja tervikluse nõuded;

4.2.2. Hävitatavad andmed kustutakse turvaliselt sellisel viisil, mis välistab nende taastamise;

4.2.3. Varundatud andmete hoidmisel rakendatakse E-ITS³ turvameetmeid, lähtudes varundatud andmete maksimaalsest turvaklassist;

4.2.4. Varundustsükli tihedus peab olema vähemalt 24 tundi;

4.2.5. Kogu lahendus peab olema taastatav mitte rohkem kui 24 tunni vanuste andmetega;

4.2.6. Tarkvara peab vastama isikuandmete kaitse üldmääruses kehtestatud (General Data Protection Regulation - GDPR) isikuandmete töötlemise nõuetele.

5. Tarkvara tööle rakendamine:

5.1. Pakkuja annab tellija esindajatele üle lahenduse juhend- ja koolitusmaterjalid, mis võimaldavad tarkvara ilma täiendava juhendamiset kasutada ja vajadusel viib tellija

² Kriitiline on probleem siis, kui teenus on märkimisväärselt häiritud, süsteem on kasutamiskõlbmatu või ei ole kõigile kasutajatele kättesaadav.

³ Eesti Infoturbestandard

esindaja(te)le läbi tarkvara ülesehitust ja kasutamist tutvustava eesti- või ingliskeelse koolituse mahus, mis on mõistlikult vajalik tarkvara liidestamiseks tellija asutuse infosüsteemidega ja kasutamisoskuste omandamiseks;

6. Muud nõuded:

- 6.1. Tarkvara peab vastama E-ITS töökindluse turvaosaklassile K2⁴ või selle ekvivalendile (töökindlus – 99% (lubatud summaarne seisak nädalas ~ 2 tundi), lubatav nõutava reaktsioonaja kasv tippkoormusel – minutid (1÷10));
- 6.2. Tarkvara peab vastama E-ITS info allika turvaosaklassile T2⁵ või selle ekvivalendile (info allikas, selle muutmise ja hävitamise fakt peavad olema tuvastatavad, vajalik on info õigsuse, täielikkuse ja ajakohasuse perioodiline kontroll);
- 6.3. Tarkvara peab vastama minimaalselt E-ITS andmete konfidentsiaalsuse turvaosaklassile S2⁶ või selle ekvivalendile (info asutusesiseseks kasutamiseks, info kasutamine on lubatud ainult teatud kindlatele kasutajate gruppidele ja juurdepääs teabele on lubatav juurdepääsu taotleva isiku teadmishajaduse korral);
- 6.4. Mitte eestikeelse tarkvara pakkujal peab olema võimekus viia kasutajaliides eestikeelseks kolme kuu jooksul alates lepingu sõlmimisest;
- 6.5. Tarkvara soetatakse teenusena (Software As A Service – SAAS), mis tähendab, et tellija ei pea tarkvara kasutamiseks omapoolset infrastruktuuri looma;
- 6.6. Tarkvara kasutuselevõtt peab olema võimalik koheselt pärast hankelepingu sõlmimist.
- 6.7. Hankega hangitakse valmis tarkvara, mitte tarkvara arendamist.

7. Kasutuslitsentsid:

- 7.1. Raamlepingu periood on 4 aastat alates lepingu sõlmimisest.
- 7.2. Kasutuslitsentsid soetatakse vastavalt tellija vajadusele.
- 7.3. Raamlepingus osaleb kokku 15 ühishankijat, neis on tänase parima teadmise põhjal kasutajaid järgmises suurusjärgus:
 - 7.3.1. Tavakasutajaid 8200;
 - 7.3.2. Dispetšer-kasutajaid 410;
 - 7.3.3. Administraator-kasutajaid 50.

⁴ Vabariigi Valitsuse 09.12.2022 määruse nr 121 „Võrgu- ja infosüsteemide küberturvalisuse nõuded“ § 10 lg 4 p 3 <https://www.riigiteataja.ee/akt/113122022030>

⁵ Vabariigi Valitsuse 09.12.2022 määruse nr 121 „Võrgu- ja infosüsteemide küberturvalisuse nõuded“ § 10 lg 5 p 3 <https://www.riigiteataja.ee/akt/113122022030>

⁶ Vabariigi Valitsuse 09.12.2022 määruse nr 121 „Võrgu- ja infosüsteemide küberturvalisuse nõuded“ § 10 lg 6 p 3 <https://www.riigiteataja.ee/akt/113122022030>