KINNITATUD
Direktori 10.02.2020
Käskkiri nr 11
Lisa 1

Muudetud:
30.05.2023. a nr 42

Nõuded arendustele v6.0

Võti	Nõude liik	Kokkuvõte	Kirjeldus	Nõude vastutav kontrollija
NA-1	Vastavus üldistele standarditele	Loodavate lahenduste X-tee teenused peavad vastama RIA x-tee juhendis toodud nõuetele. Aluseks tuleb võtta hanke välja kuulutamise hetkel kehtiv versioon.		Arendusosakond
NA-2	Vastavus üldistele standarditele	Lahendusega koos tarnitav standardtarkvara peab vastama RIK nõuetele	Kui hankes ei spetsifitseerita tarkvaralist lahendust tuleb kasutada vastaval konkreetsele vajadusel allpool toodud tarkvarade viimaseid stabiilseid versioone. Serverite operatsioonisüsteemina: 1) Linux RedHat Enterprise/Centos 2) Windows Andmebaasidena: 1) Microsoft SQL 2) Postgre SQL Veebiserverina: 1) Nginx 2) Microsoft IIS 3) Apache Rakendusserverina: 1) Tomcat Programmeerimiskeelena : 1) C# 2) Java 3) Python Kui koos tarnega tarnitakse kommertstarkvara peab selle litsents sisaldama vähemalt 5 aasta turvaparandusi	Infrastruktuuride osakond
NA-3	Vastavus üldistele standarditele	Rakendus peab olema loodud vastavalt Eesti Infoturbestandardi nõuetele. Aluseks tuleb võtta hanke väljakuulutamise hetkel kehtiva versiooni meetmeid. [30.05.2023 DK nr 42 - muudetud]		

NA-4	Vastavus üldistele standarditele	RIK põhimõte on arendada tarkvara avatult ja avaldada tarkvara vaba litsentsiga. Avaliku sektori kohustuseks on arendada tarkvara eelkõige avatult ja avaldada tarkvara vaba litsentsiga vastavalt litsentsi nõuetele.	Antud nõudes võib erandeid teha ainult juhul, kui on teisiti ette nähtud seadusega või muul tellijaga kokku lepitud põhjendatud juhul. RIKis kasutatavad levinuimad vaba tarkvara litsentsid on EUPL, GNU GPL, MIT. Valik sõltub vajadustest ja kohustustest. Litsentside litsentsitingimustes sisalduvad nõuded, mida tuleb litsentsi kasutamisel täita, on järgmised: **EUPLi** puhul on nõutav mh: 1) autoriõiguse märge päises (EUPL © Euroopa Liit 2007, 2016, mille järel on märge „Litsentsitud EUPL alusel“); 2) lähtekoodi avalikustamine Euroopa Liidu joinup virtuaalses varamus. **GNU GPL** puhul on nõutav mh: 1) autoriõiguse märge päises (Copyright © <aasta> <autori nimi>); 2) litsentsitingimustes ette nähtud teavitus töö osas garantii välistamise kohta. **MIT** puhul on nõutav mh: 1) autoriõiguse märge päises (Copyright © <aasta> <autori nimi>) koos litsentsis ette nähtud teavitusega; 2) litsentsitingimustes ette nähtud teavitus töö osas garantii välistuse kohta. Täpsemalt tuleb nõuetega tutvuda lähtudes valitud litsentsitüübi litsentsitingimustest. Valitud litsentsi litsentsitingimused esitatakse ühel või mõlemal alljärgnevatest viisidest: 1) LICENCE-fail peab olema repositooriumis avalikustatud koos tarkvara koodiga; 2) litsentsitingimuste tekst iga faili päises; 3) lisades päisesse link asukohale, kus on võimalik litsentsitingimustega tutvuda.	Projektijuht

NA-5	Arhitektuur	Rakenduse, andmebaasi ja kolmanda osapoole komponentide platvorm(id)/versioon(id) peavad olema sellised, mille eluea lõpp (EOL) pole teadaolevalt vähem kui 4 aasta pärast.	Kui on tuleb tellijaga paika panna ja kokku leppida vahetuse strateegia.	Infrastruktuuride osakond
NA-6	Arhitektuur	Tulevase ja olemasolevate infosüsteemide platvormid (rakendusserver, andmebaas, kolmanda osapoole komponendid) ja topoloogia peab olema enne reaalse arenduse algust RIK Infrastruktuuride osakonnaga kooskõlastatud.	Süsteemi jõudlus peab vastama kokkulepitud topoloogial eelanalüüsi ja lähteülesande käigus välja toodud jõudlusnäitajatele.	Infrastruktuuride osakond
NA-7	Arhitektuur	Rakendusserver peab võimaldama töötamist andmebaasiserverist eraldi serveril.		Infrastruktuuride osakond
NA-8	Arhitektuur	Rakendust peab saama ilma ümber programmeerimata liigutada erinevate domeenide ja domeeni saitide vahel	Lahendus ei tohi olla sisse kompileeritud absoluutseid URL-e.	Haldur koos infrastruktuuride osakonnaga
NA-9	Arhitektuur	Tõrkekindluse tagamiseks tuleb väliseid liidestusi kasutada nii vähe kui võimalik. Kui need on vajalikud, siis peavad nad olema võimalikult tõrkekindlad.	Liideseid peab saama konfiguratsioonist välja lülitada. Väliste liidestatud süsteemide tõrke korral ei tohi süsteem hanguda, vaid peab väljastama mõistliku (võimalikult lühikese) aja jooksul ajakohase veateate. Võimalusel tuleb töökindluse tõstmiseks kasutada asünkroonseid liideseid (ntäiteks Rahvastikuregistri, Maa-ameti infosüsteemi või Google analythicsk´i töötamast lakkamisel peab süsteemi põhifunktsionaalsus,kui süsteemi äriloogika seda võimaldab, tööle jääma).	Haldur koos infrastruktuuride osakonnaga
NA-10	Arhitektuur	Andmevahetus riigi infosüsteemi kuuluvate andmekogudega ja riigi infosüsteemi kuuluvate andmekogude vahel toimub läbi riigi infosüsteemi andmevahetuskihi (x-tee). Avaliku teabe seaduse § 43 (9) lõige 5.	Kui X-tee päringut teostab inimene, siis peab olema päringu päises autentinud kasutaja andmed.	Haldur
NA-11	Arhitektuur	Rakenduse testkeskkonnad peavad olema ühendatud test X-teega ja arenduskeskkonnad arendus X-teega.		Infrastruktuuride osakond
NA-12	Arhitektuur	Rakenduse konfiguratsiooniparameetrid tuleb ühte kohta kokku tuua nii, et nende muutmisel ei peaks rakendust uuesti kokku kompileerima (nt ühte tekstipõhisesse konfiguratsioonifaili, andmebaasi tabelisse).	Rakendus peab neid sealt ka kasutama (mitte kopeerima parameetreid käivitamisel kolmandatesse kohtadesse). Logimise seaded võivad olla rakenduse konfiguratsioonifailist eraldi ühes lisakonfiguratsioonifailis (näit Log4net).	Arendusosakond koos infrastruktuuride osakonnaga

NA-13	Arhitektuur	Rakenduse kompileerimine (saidi taaskäivitas, konfiguratsiooni muutmine vms) peaks toimuma mõistliku aja jooksul.	Mõistlikuks ajaks loetakse maksimaalselt 30 sekundit. Kui rakendus vajab indekseeritud sisu ja see pole kättesaadav, siis peab rakendus väljastama selle kohta selge teate.	Arendusosakond koos infrastruktuuride osakonnaga
NA-14	Arhitektuur	Rakendus peab olema 64-bitine.		Infrastruktuuride osakond
NA-15	Arhitektuur	Andmebaas ja rakendus peavad kasutama UTF-8 kodeeringut.	Nõue kehtib Oracle ja Postgre andmebaaside puhul.	Arendusosakond koos infrastruktuuride osakonnaga
NA-16	Arhitektuur	Failid peab katalogiseerima kokkulepitud tunnuste alusel (aasta, kuu, kuupäev).	Failisüsteemi salvestamisel ei tohi ühte kausta tekkida üle 10000 objekti (kaust või fail). Failistruktuur peab olema mõistlik (kaustu ei tohi olla rohkem kui faile) ning ei tohi tekitada märgatavat jõudluskadu.	Arendusosakond koos infrastruktuuride osakonnaga
NA-17	Arhitektuur	Kasutatav programmeerimise paradigma on objekt-orienteeritud.		Arendusosakond
NA-18	Arhitektuur	Kõik välised võtmed (Foreign Key) peavad olema indekseeritud.	Andmebaasis peab kasutama indekseid või muid meetmeid, et nõuded jõudlusele oleksid täidetud ka tulevikus (1, 3, 5 või 10 aasta pärast – vastavalt planeeritud kasutusajale). Väliseid võtmeid tuleb kasutada ka ühest andmebaasist teisele viitamisel.	Haldur
NA-19	Arhitektuur	Tuleb kasutada päringumuutujaid (Parameter Binding).	SQL päringute väljakutsumisel väljastpoolt andmebaasi, peab kasutama päringumuutujaid, et vältida SQL vahemälu fragmentseerumist (When calling SQL code from outside the database, Parameter Binding should be used to prevent SQL cache fragmentation).	Arendusosakond
NA-20	Arhitektuur	Kõigis andmebaasi tabelites peab olema defineeritud üks tehniline primaarvõti ja selle nimetus peab olema „ID“.		Haldur
NA-21	Arhitektuur	Failid ja failide indeks peavad olema replikeeritavad teise serveriruumi.	Failide hoidmise asukoht lepitakse iga kord eraldi kokku. Failide hoidmine klassikalises andmebaasis on kulukas ja seab kõrgendatud nõudmised ning piirangud andmebaasiserveritele.	Infrastruktuuride osakond
NA-22	Arhitektuur	Vajadus halduril teha otse baasis haldustoiminguid peab olema viidud miinimumini.	Rakendusel peab olema haldusliides, mille kaudu rakenduse haldur saab teha tavapäraseid haldustoiminguid. Halduri haldustoimingud lepitakse tellijaga kokku detailanalüüsi käigus.	Haldur

NA-23	Arhitektuur	Andmebaas peab toetama nii külm- kui ka kuumvaru (peegeldamist) teise serveriruumi.	Ei tohi kasutada teenuseid, mis välistavad andmebaasi peegeldamist (nt "failstream").	Infrastruktuuride osakond
NA-24	Arhitektuur	Sorteerimisreeglistik peab vastama eesti keele tähestikule.	Tõusutundlikkus peab olema välja lülitatud ning *accent* peab olema sisse lülitatud. Näiteks: MS SQL puhul Estonian_CI_AS.	Infrastruktuuride osakond
NA-25	Arhitektuur	Kui süsteem saadab elektronkirju, peab kasutama süsteemivälist RIK-i elektronposti serverit.	Kirjade tekst peab olema haldurite poolt hallatav. Kirja saatmisel peab süsteem veenduma, et elektronposti server võttis meili vastu. Kui elektronposti server millegi pärast kirju vastu ei võta, tuleb kirjad ära saata pärast seda kui elektronposti server jälle vastab. Kirjad saatmist peab olema võimalik lihtsalt (näiteks muudatuse ajaks) rakenduse konfiguratsioonist kinni keerata.	Infrastruktuuride osakond
NA-26	Arhitektuur	Konfiguratsiooniparameetrite nimed peavad olema sisulised. Juhul kui see ei ole võimalik, peab kõrval olema selgitus.	Näiteks : X-tee Turvaserver, mitte XTTS või viitenumber, mitte vk_sebjne.	Arendusosakond koos infrastruktuuride osakonnaga
NA-27	Arhitektuur	Infosüsteemides on eessüsteemid (front end) ja tagasüsteemid (back end) arhitektuuriliselt selgelt lahutatud.	Tagasüsteemide ülesanneteks on andmete haldamine ja võrguteenuste pakkumine. Tagasüsteemid ei tegele lõppkasutaja autentimise ja autoriseerimisega. Lõppkasutaja autoriseerimise tagavad eessüsteemid.	Infrastruktuuride osakond
NA-28	Arhitektuur	Konfiguratsioonifailid peavad olema vastavalt rakendusserveri tüübile vaikimisi kaitstud failid	Näiteks IIS: *.config , *.resources Apache: *.conf, .htaccess. Kui neid on mitu, siis arendaja peab need eraldi välja tooma konfiguratsioonifailide listis.	Arendusosakond koos infrastruktuuride osakonnaga
NA-29	Arhitektuur	Rakenduse failid, mida kasutaja näha ei tohi, peavad olema vaikimisi kaitstud kaustades.	Näiteks: IIS: Bin,App_Code, App_Data, App_Browsers, App_GlobalResources, App_LocalResources, App_Themes, App_WebReferences	Arendusosakond koos infrastruktuuride osakonnaga
NA-30	Arhitektuur	Konfiguratsioonis ei tohi olla erinevaid parameetreid, mis on sama sisuga.	Kõiki parameetreid tuleks konfiguratsioonis kirjeldada vaid uhe korra (mitte nii, et mitmes lõigus kirjeldatakse samu asju uuesti).	Arendusosakond koos infrastruktuuride osakonnaga
NA-31	Arhitektuur	Kõik rakendused peavad töötama kõrgkäideldavalt.	Rakendustes tohib kasutada vaid masinapõhiseid teenuseid, mis lubavad kõrgkäideldavaid (klaster) lahendusi. Kõrgkäideldav lahendus peab olema selline, mida saab samaaegselt käitada erinevates masinates. Kasutajasessioon ei tohi olla ühe klastri üle põhine. Ei tohi kasutada *sticky sessioneid.*	Arendusosakond koos infrastruktuuride osakonnaga

NA-32	Arhitektuur	Tuleb kasutada rakendusservereid.	Klientrakendus ei tohi pöörduda otse andmebaasi poole.	Arendusosakond koos infrastruktuuride osakonnaga
NA-33	Arhitektuur	Keskkonnapõhiseid muutujad peavad olema konfiguratsioonist seadistatavad.	Näiteks WSDL ei tohi sisaldada viiteid arendusserveritele.	Arendusosakond koos infrastruktuuride osakonnaga
NA-34	Arhitektuur	Kui kasutatakse Windows teenuseid peavad teenuste nimed olema serveri administraatori poolt konfigureeritavad.		Infrastruktuuride osakond
NA-35	Arhitektuur	Rakenduse äriloogika tuleb realiseerida eraldi andmebaasist sõltumatus rakenduskihis.	Andmebaas ei tohi sisaldada äriloogikat, mis muudab andmetabelites olevaid ja sinna kirjutatavaid andmeid. Erandiks on trigerid, mis tekitavad logi.	Arendusosakond
NA-36	Arhitektuur	Andmebaasis võib kasutada vaid ISO/IEC 9075 standardiga kaetud funktsionaalsusi. Kuid erandina ei tohi kasutada sama standardi osas 13 kirjeldatud funktsionaalsusi.	Ei ole tohi kasutada selliseid platvormispetsiifilist lahendusi, mille üleviimine mõnele muule andmebaasiplatvormile ei ole võimalik. ISO/IEC 9075 osa 13 spetsifitseerib Javas kirjutatud programmimoodulite kasutamist andmebaasis.	Arendusosakond
NA-37	Arhitektuur	Rakendus peab kasutama autentimiseks RIK autentimisportaali AUP.	RIK kasutab keskset autentimislahendust (AUP). Kui kui mõni ärinõue välistab AUP kasutamise, esitab RIK arendajale lisanõuded autentimissüsteemile. Kasutatavaid autentimisviise peab olema rakenduse konfiguratsioonist võimalik sisse ja välja lülitada. Samuti peab rakenduse konfiguratsioonist olema määratav kas ID-kaardiga autenimise korral kasutatakse OCSP või tühistusnimekirjade põhist autentimist.	Haldur koos infrastruktuuride osakonnaga
NA-38	Arhitektuur	Uniform resource identifier (URI) pikkus ei tohi ületada ühegi IS poolt toetatava brauseri maksimaalset lubatud väärtust.	Max uri < 2000.	Haldur koos arendusosakonnaga
NA-39	Arhitektuur	Rakenduse teenusekirjeldus (n: WSDL) peab olema üles ehitatud nii, et see toetaks teenuse versioneerimist.	Näiteks: Alajaotis definitions/types/schem: complexType defineerimisel tuleb sellele lisada "any" element.	Arendusosakond

NA-40	Arhitektuur	Rakenduse operatiivbaas peab olema võimalikult väike.	Juhul kui äriprotsess seda võimaldab, tuleb suurte andmemahtude korral kasutada andmete arhiveerimist põhibaasist väljapoole.	Arendusosakond koos infrastruktuuride osakonnaga
NA-41	Arhitektuur	Rakendusega tarnitavad litsentsid peavad olema vähemalt 5 aastase kehtivusega.	EU projektide korral tuleb kehtivusaja suhtes lähtuda EU või RIA nõuetest.	Infrastruktuuride osakond
NA-42	Arhitektuur	Rakendus peab olema tehniliselt osadeks jaotatud (tükeldatud) vastavalt loogilisele jaotusele. Saadud osised peavad olema eraldi versioneeritavad ja paigaldatavad.	Eraldatud peavad olema teenused, kuhu pöörduvad kasutajad ja need teenused, kuhu pöörduvad teised teenused ja serverid (näiteks saidid). Avalikud liidesed tuleb selgelt eristada muudest mitteavalikest, sisemistest, konfigureerimis jms liidestest. Kui rakendusel on eraldi turvatasemega liidesed ametnikule ja kodanikule, peab rakendus olema jaotatud kaheks eraldi liidesekomponendiks ning nende mõlema poolt kasutatavaks andmebaasiks.	Arendusosakond
NA-43	Arhitektuur	Kõik dokumentide konverteerimised ühest formaadist teise tuleb teha kasutades RIK keskseid dokumentide konverteerimise teenuseid.		Arendusosakond
NA-44	Arhitektuur	Süsteem ei tohi võimaldada kasutajale ligipääsu süsteemi toimimise informatsioonile, nagu failide täisnimed (path), kutsepinud (stack trace) jms.		Haldur koos arendusosakonnaga ja infrastruktuuride osakonnaga
NA-45	Arhitektuur	Rakendus peab olema võimeline töötama koormusjaoturitega varustatud taristul.	SSL offload, vajalike kliendiparameetrite edasiandmine kasutades http headereid.	Arendusosakond koos infrastruktuuride osakonnaga
NA-46	Arhitektuur	Rakenduse failidele ei tohi olla rohkem ligipääsuvajadust, kui read-execute.		Arendusosakond koos infrastruktuuride osakonnaga
NA-47	Arhitektuur	Kui on planeeritud kasutada Windows servereid peavad kõik rakenduse osad (ka baas) olema võimelised töötama windows core serveritel.		Infrastruktuuride osakond
NA-48	Arhitektuur	Andmebaasis tuleb veerutüübiks määrata selleks sisuliselt sobivaim andmetüüp.	Näiteks, kui on tegemist kuupäevaga, siis date. Kasutada ei tohi varchar(max) andmetüüpi, kui see pole põhjendatud ja vajalik.	Haldur

NA-49	Arhitektuur	Rakendus peab väljastama oma masinliideste teenuste tehnilisi spetsifikatsioone.	SOAP teenuste wsdl'e, REST teenustele n:swaggeri v. openapi formaadis kirjeldusi.	Haldur koos arendusosa konnaga
NA-50	Arhitektuur	Active Directory (AD) autentimise kasutamisel peab rakendus kasutama SAML2.0 (Security Assertion Markup Language) ja ADFS (Active Directory Federation Services) standardeid.	Teiste standardite kasutus tuleb RIK-iga eelnevalt kooskõlastada.	Infrastruktuuride osakond
NA-51	Arhitektuur	ID-kaardiga (kliendi sertifikaadiga) autentimist teostavad veebirakendused peavad (juhul, kui sessiooni pole algatatud) suhtlema kliendi veebirakendusega ainult selleks, et saada veebirakendusest sisselogimiseks vajaliku koodi.	Edasine koodi täitmine ja võimalike veaolukordade töötlus peab toimuma rangelt ainult kliendi poolel. Kliendi autentimissertifikaadi kehtivus- ja autentsusekontroll teostatakse maksimaalses võimalikus mahus veebiserveri või proxy poolt. Autentimissertifikaadil on veebiserveri või proxy poolt kohustuslikult nõutav: Apache: SSLVerifyClient require; NGINX: ssl_verify_client on; Pulse TM: ssl.requireCert(); HAProxy: verify required; Tomcat: clientAuth="true"; jne… Juhul kui toimub pöördub URL poole, kus on nõutud kliendi autentimissertifikaat ning server vastab veaga, peab klientrakendus kuvama korrektse eesti keelse veateate. NB! Rakenduse javascrip-ti tuleb ID-kaardiga autentimise puhuks erand kirjutada!	Infrastruktuuride osakond
NA-52	Arhitektuur	Tuleb kasutada vaid RIK poolt ette antud captcha lahendust.		
NA-53	Arhitektuur	Rakendustevaheline suhtlus tuleb realiseerida läbi rest- või soap-vms veebiteenuste või message queue.	Sobivad liideste formaadid lepitakse kokku projekti käigus.	
NA-54	Arhitektuur	Serveris peab olema kirjeldatud, millistele HTTP meetoditele vastatakse.	Mitte kirjeldatud meetoditele ei tohi vastata.	
NA-55	Arhitektuur	Vigastele meiliaadressidele ei tohi kirju saata.	Meiliaadress peab vastama RFC5322 ja/või RFC6854 standardile. Süsteem, kuhu on võimalik e-posti aadresse sisestada, peab kontrollima nende kehtivust. Kasutaja kontaktinfo tuleb alati valideerida.	

NA-56	Arhitektuur	Rakendusel peab olema CSP header. Vaikeväärtus on "self".	Erandid tuleb kirjeldada pigaldusjuhendis.	
NA-57	Turvalisuse ja terviklikkuse tagamisega seotud nõuded	Kliendi ja serveri vaheline side peab olema krüpteeritud SSL-protokolli kasutades.	Tuleb arvestada tingimusega, et osad ühendused nõuavad kahepoolset SSL autentimist (nt: suhtlus turvaserveriga).	Haldur koos infrastruktuuride osakonnaga
NA-58	Turvalisuse ja terviklikkuse tagamisega seotud nõuded	Rakendus ei salvesta andmeid kliendi arvutisse (sh küpsiseid).	Erandiks on mitmekeelse süsteemi puhul keelevalik.	Arendusosakond
NA-59	Turvalisuse ja terviklikkuse tagamisega seotud nõuded	Sessiooni lõpetamine infosüsteemis (nt logi välja nupu vajutamine) peab serveri poolt sessiooni tunnused kehtetuks tunnistama (nt küpsised).		
NA-60	Turvalisuse ja terviklikkuse tagamisega seotud nõuded	Kui andmebaasis olevate andmete turvaosaklass "terviklus" on 2 või 3, tuleb kõik osaklassi 2 või 3 infot sisaldavad andmebaasi kirjed ja tabelid versioneerida. [30.05.2023 DK nr 42 - muudetud]	Kõik andmemuudatused peavad baasis säilima. Andmete muutmisel andmeid ei kustutata, vaid tehakse uus kirje uute andmetega. Vana kirjed muudetakse kehtetuks. Iga uus kirje peab sisaldama vähemalt järgmist informatsiooni: 1) viide kirjele, mille ta kehtetuks muutis (kui on); 2) kasutaja, kes kirje lõi; 3) kirje loomise aeg; 4) sessiooni-ID (kui on olemas). Iga kehtetuks tunnistatud kirje peab sisaldama lisaks vähemalt järgmist informatsiooni: 1) kasutaja, kes kirje kehtetuks tunnistas; 2) kirje kehtetuks tunnistamise aeg.	Haldur
NA-61	Turvalisuse ja terviklikkuse tagamisega seotud nõuded	Kui rakenduse poolt töödeldavate andmete konfidentsiaalsusklass on 2 või kõrgem, peab rakendusega kaasas olema lahendus, mis suudab toota toodangu andmetest testandmed, mis ei sisalda konfidentsiaalset informatsiooni.	Testandmed peavad säilitama kõik toodangu andmete omadused (pikkuse, tüübi) ja omavahelised suhted. Toodanguandmetest testandmete tegemise algoritmid ja põhimõtted tuleb eelnevalt kooskõlastada tellijaga.	Haldur
NA-62	Turvalisuse ja terviklikkuse tagamisega seotud nõuded	Andmebaasis olevate rakenduse kontod peavad omama ainult minimaalselt rakenduse tööks vajalikke õiguseid.	Schema muutmine ei ole rakenduse töö. Schema omanik ei tohi olla rakenduse tööks kasutatav baasi kasutaja. Nõude täitmiseks vajalikud vahendid (skriptid) peavad kuuluma rakenduse juurde ja nende sisu peab olema kontrollitav. Kontodele vajalikud õigused peavad olema kirjeldatud rakenduse installatsioonijuhendis.	Infrastruktuuride osakond

NA-63	Turvalisuse ja terviklikkuse tagamisega seotud nõuded	Rakenduse lõppkasutajatele peab olema võimalik jagada õigusi läbi andmebaasis defineeritud rollide.	Rakendusepõhiseid kasutajarolle ei tohi defineerida ainult läbi AD OU'de ja gruppide.	Haldur
NA-64	Turvalisuse ja terviklikkuse tagamisega seotud nõuded	Ligipääs rakendusse ja andmetele tohib olla vaid dokumenteeritud ning tellimuses kirjeldatud teid mööda ja dokumenteeritud autentimisprotseduure kasutades.		Arendusosakond
NA-65	Turvalisuse ja terviklikkuse tagamisega seotud nõuded	Kõik paroolid ja salasõnad peab rakendus alati salvestama vaid krüpteeritud või räsitud ja soolatud kujul.	Räsimine peab kasutama turvalist räsifunktsiooni (NA-74) ja soola (salt). Sool peab olema andmebaasiüleselt unikaalne, piisavalt suure bitiarvuga ja "random". Krüpteerimata kujul ei tohi paroole salvestada (ka ajutiselt) ühelegi kettale. Krüpteering peab olema CBC, CRT vms režiimis. Kasutada ei tohi ECB režiimi.	Arendusosakond
NA-66	Turvalisuse ja terviklikkuse tagamisega seotud nõuded	Rakendused, kuhu saavad ligi välised kasutajad, peavad võimaldama autentimist vähemalt kahe erineva Eesti riigi poolt aktespteeritava kaheastmeilse isikutuvastsulahendusega. Parooliga autentimsit tuleb vältida.	Kindlasti peab olema kasutusel ID-kaardi põhine autentimine. Kui on vajalik ka parooliga logimine, peavad välised kasutajad autentima ennast spetsiaalse väliskasutajate jaoks mõeldud AD pihta. Mingil juhul ei tohi väliskasutajaid teha RIK-i sisemisse AD-sse.	Haldur
NA-67	Turvalisuse ja terviklikkuse tagamisega seotud nõuded	Rakendus ei tohi teostada X-tee päringut otse kasutajaarvutist.	Kasutajaarvutitest otse x-tee päringute tegemine on arvutivõrgu tasemel keelatud.	Arendusosakond
NA-68	Turvalisuse ja terviklikkuse tagamisega seotud nõuded	Veebipõhised välise veebilehega rakendused, mis on keskmise või kõrgema ISKE klassiga peavad kasutama vahendeid kaitsmaks rakendust keelatud päringute eest.	IIS puhul peab kasutama näiteks URL scan, apache puhul modsecurity või vastavat tööriista. Võimalikud piirangud tuleb kokku leppida tellijaga detailanalüüsi käigus lähtuvalt tellija vajadustest ja nõudmistest. Kasutama peab whitelisting põhimõtet, mitte blacklistingut.	Arendaja koos Infrastruktuuride osakonnaga
NA-69	Turvalisuse ja terviklikkuse tagamisega seotud nõuded	Kui rakenduse kaitsetarve on suur või väga suur, peab rakendus sisenemisel näitama pärast õnnestunud sisselogimist eelmise õnnestunud sisselogimise aega. [30.05.2023 DK nr 42 - muudetud]	Sarnaselt õnnestunud sisselogimisega, tuleb ebaõnnestunud sisselogimise katsete korral kuvama millal need toimusid ja mitu neid oli. Kasutaja peab saama soovi korral veenduda, kas keegi pole tema nime all üritanud sisse logida. ID-kaardi, mobiil-ID ja digi-ID-ga sisenemise ürituse ebaõnnestunud katseid näitama ei pea.	Haldur

NA-70	Turvalisuse ja terviklikkuse tagamisega seotud nõuded	Rakenduse kasutajaliidesest peab olema kasutajal avalehel ilma sisse logimiseta võimalik näha rakenduse versiooni numbrit.	Mõeldud on spetsiaalrakendusi (custom built). Nõue ei kehti veebitarkvara (apache, IIS jne), andmebaaside jms kohta. Viimaste versiooni numbrit tuleb pigem varjata.	Haldur
NA-71	Turvalisuse ja terviklikkuse tagamisega seotud nõuded	Sessioonide lõpetamine tuleb teostada serveri poolel ja kõigil rakendustel peab olema konfigureeritav kasutajasessiooni aegumise aeg.	Aeg peab olema muudetav koos teiste konfiguratsiooniparameetritega. Kui kliendilt pole etteantud aja jooksul ühtegi päringut tulnud, tuleb sessioon serveri enda algatusel lõpetada.	Infrastruktuuride osakond
NA-72	Turvalisuse ja terviklikkuse tagamisega seotud nõuded	Veebipõhiste rakenduste mitteautentinud kasutajate poolt saadetud vormid tuleb puhastada XSS-filtriga või eemaldada HTML-tag´id.	Soovitatavalt tuleb seda teha enne andmebaasi salvestamist, vajadusel andmete väljakuvamisel.	Arendusosakond koos infrastruktuuride osakonnaga
NA-73	Turvalisuse ja terviklikkuse tagamisega seotud nõuded	Veebipõhiste rakenduste poolt saadetavad vormidel peab paiknema peidetud unikaalne räsi, mida kontrollitakse vormi vastuvõtmisel.	Eesmärk on vältida CSRF rünnakuid.	Arendusosakond koos infrastruktuuride osakonnaga
NA-74	Turvalisuse ja terviklikkuse tagamisega seotud nõuded	Krüpteerimise ja räside arvutamise korral tuleb kasutada tugevaid algoritme.	Valida tohib vaid neid, mille soovituslik kasutusaeg RIA krüptoprotokollide elutsükliuuringu uuringu kohaselt on üle 12 aasta. Kui räsimine ei pea tagama pikaajalist salastaatust ja tõestusväärtust võib tellijaga kokkuleppel kasutada algoritme, mille soovituslik kasutusaeg on krüptoprotokollide elutsükliuuringu uuringu kohaselt üle 5 aasta. Kui tehniliselt vähegi võimalik tuleb sertifikaate hoida RIK HSM lahenduses. Ligipääs võtmetele ja sertifikaatidele peab olema vaid teadmisvajaduse põhimõttel. Kirjandus: NIST SP-800-57 Key Management Guidelinesja European Payments Council (2017) Guidelines on cryptographic algorithms usage and key management. Süsteemi kirjelduses tuleb välja tuua kõik krüptoalgoritmid, võtmepikkused ja kasutuskohad.	Arendusosakond
NA-75	Turvalisuse ja terviklikkuse tagamisega seotud nõuded	Autenditud sessiooni tunnust ei tohi ainult lihtsa küpsisega lahendada (kasutada OWASP parimaid praktikaid).	Sessiooni ei tohi olla võimalik üle võtta URLi kopeerimisega ühest arvutist teise.	Arendusosakond

NA-76	Turvalisuse ja terviklikkuse tagamisega seotud nõuded	Halduritel ei tohi olla võimalik muuta rakenduseväliste liidestuste-ning nendega seotud äriloogiliste funktsionaalsuste tehnilisi konfiguratsioone.	Tagada tuleb rollide lahusus: administraatoril ja halduril on erinevad tööülesanded.	Haldur koos infrastruktuuride osakonnaga
NA-77	Turvalisuse ja terviklikkuse tagamisega seotud nõuded	ID-kaardiga autentimisel, peab rakendus suutma vastu võtta ID-kaardi sertifikaati ka HTTP päises.	Proxy tugi	Arendusosakond koos infrastruktuuride osakonnaga
NA-78	Turvalisuse ja terviklikkuse tagamisega seotud nõuded	Kõik digitembeldamist vajavad rakendused peavad kasutama RIK-i-keskset digitembeldamise teenust.		Arendusosakond
NA-79	Turvalisuse ja terviklikkuse tagamisega seotud nõuded	Rakenduse turvalisuse tagamiseks (näiteks XSS, SQLInjection, jne) tuleb järgida OWASP-i parimaid praktikaid.	Veebirakendus peab probleemideta läbima OWASP ASVS põhineva testi. Esmane väline turvatestimine tellitakse tellija finantseeringul. Kui selle tulemusel leitakse arendaja poolsest tegevusest või tegevusetusest põhjustatud vigu, võib tellija nõuda OWASP järeltestide kompenseerimist arendajalt.	Arendusosakond koos infrastruktuuride osakonna ja sisekontrolli- ja infoturbe osakonnaga
NA-80	Turvalisuse ja terviklikkuse tagamisega seotud nõuded	Arendus peab olema orienteeritud toodangukeskkonnas toimimiseks.	Toodangukeskkonna rakendus ei tohi sisaldada osiseid, mis on toodangu keskkonnas ebavajalikud või segavad (näiteks mõeldud testimiseks testkeskkonnas, arendusabiks arenduskeskkonnas jne).	Arendusosakond
NA-81	Turvalisuse ja terviklikkuse tagamisega seotud nõuded	Ajatemplite kasutamisel eelistatakse Guardtime lahendust.	Ajatempli serveri URL peab olema konfigureeritav.	Arendusosakond koos infrastruktuuride osakonnaga
NA-82	Turvalisuse ja terviklikkuse tagamisega seotud nõuded	Rakendus ei tohi lubada ühe kasutajaga mitut samaaegset sessiooni.	Nõue ei kehti, kui see tellija poolt eraldi ärinõuetes nõutud.	Haldur

NA-83	Turvalisuse ja terviklikkuse tagamisega seotud nõuded	Kui rakenduse tervikluse turvaosaklass on T3, peavad tõestusväärtust omavad andmed olema digitaalallkirjastatud või digitembeldatud. [30.05.2023 DK nr 42 - muudetud]	Konkreetne lahendus valitakse ja lepitakse tellijaga eraldi kokku. Käesoleva nõude täpsustuseks vt ISKE nõue HT.34. Ajatemplite, digitemplite ja digitaalallkirjade terviklust tuleb reaalajas ja hiljem perioodiliselt (muudetava perioodiga) valideerida. Valideerimise protsessi tulemusena tuleb genereerima automaatne raport, mis on vaadeldav süsteemi halduri liidese kaudu ning mida on võimalik automaatselt edastada ettenähtud e-posti dressidele. Raport peab sisaldama infot valideerimise protsessi alguse ja lõpu aja kohta, infot selle kohta, kui mitut ajatemplit kontrolliti ja kas infot kõik ajatemplid olid korrektsed. Kui tembeldamises või allkirjastamises ilmneb viga, peab olema võimalik hiljem katkenud kohast tembeldamist või allkirjastamist jätkata.	Haldur koos arendusosa konnaga
NA-84	Turvalisuse ja terviklikkuse tagamisega seotud nõuded	Kui rakenduse tervikluse turvaosaklass on T3, peavad tõestusväärtust omavad andmed ja logid olema krüptoaheldatud, et tagada, et tõestusväärtusega andmeid ei saaks märkamatult kustutada. [30.05.2023 DK nr 42 - muudetud]	Ahela moodustamiseks ei tohi kasutada andmetesse kirja pandud viiteid (n: id=2ja andmed="mingid andmed", eelmine_andmed=1). Krüptoahela koostamisel tuleb kasutada lahendust, kus järgmise ajatembeldatava kirje koosseisu fikseeritakse eelmise kirje mitte ajatembeldatud räsi. Uue ahela lüli lisamisel tuleb kontrollida eelmise lüli korrektsust. Tagatud peab olema ka nõue, et kirjeid ei saaks märkamatult kustutada ahela lõpust. Krüptoahela terviklust peab saama perioodiliselt (muudetava perioodiga) kontrollida ja lahendus peab suutma vajadusel and häire (e-kiri) kui terviklus on kompromiteeritud. Krüptoaheldamis e ja selle kontrolli sisse ja väljalülitamine ning kontrolliperioodi muutumiine peab olema teostatav vaid rakenduse konfiguratsioonist rakenduse administraatori poolt,	Haldur koos arendusosa konnaga
NA-85	Turvalisuse ja terviklikkuse tagamisega seotud nõuded	Kui rakenduses on S3 salastatuse astmega andmeid, peavad need nii transpordil kui ka salvestatult alati olema krüpteeritud kujul.	Sümmeetrilise võtme turvamiseks tuleb kasutada asümmeetrilisi algoritme. Sertifikaati tuleb hoida nii, et see oleks kättesaadav rakendusele, kuid mitte rakendusserveri administraatorile. Sertifikaat peab olema vahetatav, st krüptograafia edasi arenedes peab olema võimalik kasutusele võtta tugevam sertifikaat.	Arendusosa kond

NA-86	Turvalisuse ja terviklikkuse tagamisega seotud nõuded	Paksu kliendi korral ei tohi rakendus kasutaja tööjaama jätta maha krüpteerimata kujul ajutisi faile, mis sisaldavad või võivad sisaldada konfidentsiaalset või kõrget terviklust nõudvat informatsiooni.	Kui paks klient kasutab ajutisi faile, tuleb tagada nende perioodiline kustutamine tagamaks, et ei koormata liigselt kasutaja arvutit. Eesmärk on tagada, et rakenduse sulgemisel ei jääks kasutaja arvutisse maha informatsiooni, mida sinna jääda ei tohiks.	Haldur koos arendusosa konnaga
NA-87	Turvalisuse ja terviklikkuse tagamisega seotud nõuded	Rakendus peab serverist kustutama kõik ajutised failid koheselt, kui neid enam ei kasutata.	Kui kasutatakse ajutiste failide kausta peab selle asukoht olema konfiguratsioonist konfigureeritav.	Arendusosa kond koos infrastruktuu ride osakonnaga
NA-88	Turvalisuse ja terviklikkuse tagamisega seotud nõuded	Rakendus tohib aktsepteerida vaid sessioonivõtmeid, mida ta ise on väljastanud. Sisselogimisel peab kasutaja saama uue sessiooni võtme ning endine võti tuleb kehtetuks tunnistada.		Arendusosa kond
NA-89	Turvalisuse ja terviklikkuse tagamisega seotud nõuded	Kui rakendusse laaditakse faile kasutaja poolt, peab need failid valideerima (kontrollima faili tüüpi, suurust). Failid peavad läbima viirusetõrje.	Faili nimes tuleb lubada vaid suur- ja väiketähti, numbreid, "_" ja "-" ning vaid ühte punkti järjest. Viirusetõrje lahenduse pakub välja RIK infrastruktuuride osakond. Võimalusel tuleb teha tüübi ja faili laiendi vastavuse kontroll.	Haldur koos arendusosa konnaga
NA-90	Turvalisuse ja terviklikkuse tagamisega seotud nõuded	Kui rakendusse laetakse faile peab faili nimi salvestamisel sisaldama random komponenti nii, et faili tee ei ole lihtsalt ära arvatav.		Arendusosa kond koos infrastruktuu ride osakonnaga
NA-91	Turvalisuse ja terviklikkuse tagamisega seotud nõuded	Rakendus ei tohi lubada ennast kasutada iframe sees.	Iframe-i kasutamine pole lubatud ja HTTP päringutele tuleb lisada "X-Frame-Options: DENY" päis.	
NA-92	Turvalisuse ja terviklikkuse tagamisega seotud nõuded	Sessiooni küpsised peavad olema turvatud.	Sessiooni küpsise korrala tuleb lisada lipud Secure, HttpOnly ja SameSite. Küpsise nime prefiks peab olema "__Host-".	Infrastruktuu ride osakond
NA-93	Logimine, debuggimine, testimine	Rakenduse kõik üleantavad versioonid peavad enne tellijale üle andmist olema testitud.	Testplaan ja testitulemused tuleb edastada tellijale koos rakenduse üleandmisega. Nõuded testimisele RIK dokumendis "Arendamise tavad ja töökorraldus".	Haldur
NA-94	Logimine, debuggimine, testimine	Turvalisuse seisukohalt kriitilised sündmused, nagu sessiooni algamine ja lõppemise, rolli muutumine jne tuleb logida.	Vastav logi peab asuma teistest logidest eraldi failis ja andmebaasis turvalogide tabelis. Väliste rakenduse puhul tuleb logida võimalusel kasutaja IP. Sessiooni võtmete väärtuses, privaatvõtmeid ja kasutaja salasõnad võivad logisse jääda vaid räsitud kujul.	Haldur

NA-95	Logimine, debuggimine, testimine	Rakendus peab suutma logida kõiki väliste süsteemidega vahetatavaid (ka X-tee teenuste kaudu liikuvaid) pöördumisi andmevahetuslogisse.	Peab olema võimalus antud logimist välise süsteemi kaupa sisse-välja lülitada. Logi peab olema struktureeritud selliselt, et päring ja vastus on eraldi failides. Logimine peab olema võimalik nii andmebaasi kui ka failisüsteemi (iga sõnum eraldi faili, failid vähemalt päeva kaupa eraldi kaustas) või mõlemasse korraga. Logifaili asukoht peab olema administraatori poolt ilma rakendust uuesti kompileerimata seadistatav.	Haldur koos infrastruktuuride osakonnaga
NA-96	Logimine, debuggimine, testimine	Kui rakenduse turvaosaklass "konfidentsiaalne" on 2 või 3, peab tagama konfidentsiaalsuse osaklassiga 2 ja 3 andmete vaatamise logimise. [30.05.2023 DK nr 42 - muudetud]	Logi salvestatakse kasutaja tegevuse logisse. Logi peab sisaldama (toodud järjekorras) millal tehti, kasutaja ID ja isikukood (firma registrikood), kui võimalik kust tehti (seadme nimi, IP, sertifikaat), mis tegevused andmetega tehti ja kas tegevus õnnestus. Kui võimalik siis päringu SQL lause. Logida peab olema võimalik ka konkreetseid andmed, mida kasutaja serveri arvates nägi. Viimane peab aga olema välja lülitatav või asendatav põhiobjektide ID-dega päringu liikide kaupa. Logida tuleb ka kasutajate tegevuste ebaõnnestumised (näiteks õiguste puudumise tõttu). Vastav logi peab asuma tegevuslogi andmebaasi tabelis. Logimise konfiguratsioon peab olema muudetav vaid uue rakenduse paketiga (deploy). Näiteks IOC konteinerist konfigureeritav (late binding).	Haldur
NA-97	Logimine, debuggimine, testimine	Kui rakenduse turvaosaklass "terviklus" on 2 või 3, peab tagama tervikluse osaklassiga 2 ja 3 andmete loomise, muutmise ja kustutamise logimise. [30.05.2023 DK nr 42 - muudetud]	Logi salvestatakse kasutaja tegevuse logisse. Logi peab sisaldama (toodud järjekorras) millal tehti, kasutaja ID ja isikukood (firma registrikood), kui võimalik kust tehti (seadme nimi, IP, sertifikaat), mis tegevused andmetega tehti ja kas tegevus õnnestus. Kui võimalik siis päringu SQL lause. Logida tuleb ka kasutajate tegevuste ebaõnnestumised (näiteks õiguste puudumise tõttu). Vastav logi peab asuma tegevuslogi andmebaasi tabelis. Logimise konfiguratsioon peab olema muudetav vaid uue rakenduse paketiga (deploy). Näiteks IOC konteinerist konfigureeritav (late binding).	Haldur

NA-98	Logimine, debuggimine, testimine	Rakendus peab logima kõiki rakenduses tekkivaid tehnilisi vigu süsteemi logisse.	Süsteemi logid peavad asuma teistest logidest eraldi failis ja andmebaasi süsteemi logide tabelis. Logi peab sisaldama minimaalselt (toodud järjekorras) vea tekkimise aega, veakoodi, veakirjeldust (stack trace, traceback vms), võimalusel kasutaja andmeid (nimi, ID, IP ja URL), HTTP-, GET- ja POST-parameetrid ja nende väärtusi. Kas logitakse baasi või faili või mõlemasse peab olema rakendust uuesti kompileerimata administraatori poolt muudetav.	Haldur koos infrastruktuuride osakonna ja arendusosakonnaga
NA-99	Logimine, debuggimine, testimine	Failisüsteemi logimise korral peavad logid olema ka katalogiseeritud (näiteks liigi järgi) ja tunnustatud faililaiendiga (näiteks .log, .txt, .xml). Logi peab olema roteeruv, et ei tekiks liiga suuri faile või faile kus on vaid üksikuid logikirjeid.	Peab olema võimalus logimist välise süsteemi kaupa sisse-välja lülitada. Ei tohi esinda olukorda, kus ühte kausta tekib rohkem kui 10000 faili. Peab tagama, et iga rakendusserver saaks vajadusel kirjutada logid oma logifaili. Logifaili asukoht peab olema administraatori poolt ilma rakendust uuesti kompileerimata seadistatav.	Infrastruktuuride osakond

NA-100	Logimine, debuggimine, testimine	Kogu rakenduse logi peab olema ühesuguse formaadiga, kergesti masinloetav ja täielik (kes, mis, mida, jms). Logis ei tohi kasutada klassifikaatoreid.	Logiväljad, mida lõppkasutaja saab manipuleerida (IP, useragent, URL) peavad salvestuma logisse kodeeritud kujul. Tuleb võimalusel vältida olukorda, kus ühe päringu tõttu tekib kirjeid mitmesse logisse. Igas logikirjes peab olema päringu unikaalne identifikaator, mis võimaldab logikirjet siduda teiste logikirjetega, mis tekkisid sama päringu tagajärjel. Seda nii ühe faili piires, kui ka juhul kui päringu tulemusel kirjutati mitmesse logi asukohta.. Sama infot sisaldavad väljad peavad (ka erinevates) logiasukohtades olema sama nimega ja andmed samas formaadis. Failisüsteemis asuv logi peab olema XML, JSON või CSV formaadis. Kui parameetri väärtus on tühi, tuleb see logis märkida asendusväärtusega (nt “null”). Kui vähegi võimalik peab logi kuupäeva ja ajaformaat olema kujul "AAAA-KK-PP ja hh:mm:ss,nnnn“ lokaalne Eesti ajavöönd. "hh" järgib 24-tunnist kellaajaformaati. Kuupäev ja kellaaeg samas andmeväljas esitatakse kujul, kus kuupäevavormingu ja kellaajavorming vahele lisatakse täht T.	Haldur
NA-101	Logimine, debuggimine, testimine	Logi tabelid peavad olema arhiveeritavad operatiivbaasist välja.	Tabeli suurenedes peab olema võimalik hoida vanu kirjeid, näiteks kuude või aastate kaupa, iseseisvates tabelites või teises baasis. Mehhanism peab töötama ka krüptoaheldatud logi korral.	Haldur koos infrastruktuuride osakonnaga
NA-102	Logimine, debuggimine, testimine	Kui rakendus kasutab või pakub väliseid teenuseid (näiteks SK teenuseid) peab ta suutma arvestust pidada vastavate teenuste kasutamise mahu üle.	Näiteks kui palju on kasutatud kuus, aastas jne digitembeldamist, ID-autentimist, autentimisportaali, pangalingi kasutamist jne.	Haldur
NA-103	Logimine, debuggimine, testimine	Rakendusega peab olema kaasas skript jõudlustestide tegemiseks.	Jõudlustestide täpne kirjeldus tuleb kokku leppida detailanalüüsi käigus. Arendaja peab koos rakendusega tarnima skripti ja vajalikud tarkvaralised vahendid kokkulepitud jõudlustestide läbiviimiseks. Jõudlustestide läbiviimine ei tohi nõuda tellijalt omapoolset tarkvara arendamist, skriptide kirjutamist või litsentside ostmist.	Haldur koos infrastruktuuride osakonnaga

NA-104	Logimine, debuggimine, testimine	Rakendusel peab olema masinloetav XML-staatusleht, mille struktuur vastab tellija poolt ette antud XML struktuurile.	Staatuslehe nõuded sisalduvad käesoleva dokumendi lisas 1.	Haldur
NA-105	Nõuded lähetkoodile ja paigaldamisele	Lähtekoodi kommentaarid peavad kõigis lahenduse kihtides (rakenduse enda kood, andmebaas, jne) olema kirjutatud eesti keeles.	Nõuet ei arvestata arendustarkvara poolt automaatselt genereeritavate koodilõikude puhul. Samuti ei rakendata nõuet kolmandate osapoolte poolt toodetud lähtekoodile – nt: erinevad lahtise koodiga kooditükid jne.	Arendusosa kond
NA-106	Nõuded lähetkoodile ja paigaldamisele	Rakenduse kood peab olema piisavalt hästi kommenteeritud, et erialast haridust omav tarkvaraarendaja on võimeline süsteemile jätkuarendusi teostama.	Lähtekoodi kommentaarid peavad olema: 1. Põhjendatud. Kommenteerida ainult kommenteerimise pärast pole vaja. Kood peab olema kirjutatud selliselt, et see on loetav ka ilma kommentaarideta. Kommentaarid on mõeldud keeruliste ja/või kohendamist ja/või edasist tööd (viimaste juurde on tuleks märkida TODO) vajavate kohtade jaoks. 2. Aktuaalsed - kommentaar ja kood peavad olema üksteisega vastavuses. 3. Selged ja üheselt mõistetavad. 4. Korrektselt kirjutatud - grammatika ja lauseehitus peavad olema korrektsed.	Arendusosa kond
NA-107	Nõuded lähetkoodile ja paigaldamisele	Muutujate, tüüpide ja funktsioonide nimed peavad olema sisulised ja andma selget informatsiooni nende otstarbest.		Arendusosa kond
NA-108	Nõuded lähetkoodile ja paigaldamisele	Koodis kasutatavaid konstante ei tohi väärtusena hardcodeda – need tuleb defineerida muutujatena ja kasutada läbi nende.		Arendusosa kond
NA-109	Nõuded lähetkoodile ja paigaldamisele	Koodis defineeritud andmetüübid peavad olema nimetava käände ainsuses. Kõik andmemassiivid tuleb nimetada nimetava mitmuses (näiteks collectionid, arrayd, jms).	Näiteks "Isik", "Menetlus" jne. Andmebaasides ei tohi kasutada täpitähti.	Arendusosa kond
NA-110	Nõuded lähetkoodile ja paigaldamisele	Andmetabelites sisalduvad võõrvõtmed peavad nime järgi seostuma tabeli ja väljaga millele need viitavad.	Näiteks kui on tegu tabelitega 'Isikud' ja 'Autod', siis seos 'isiku autod' oleks: Isikud.ID=Autod.Isik_ID	Haldur
NA-111	Nõuded lähetkoodile ja paigaldamisele	Andmebaasi väljade pikkused tuleb kirjeldada tähemärkides.	Näiteks Oracle korral Nvarchar(2000) tähendab 2000 baiti mitte tähemärki.	Haldur
NA-112	Nõuded lähetkoodile ja paigaldamisele	Kui kokku pole lepitud teisiti, siis JAVA rakenduse kood peab olema kirjutatud vastavalt "SUN Java Code convention" dokumendile.	Valideerimiseks kasutatakse 'checkstyle' vaikimisi konfiguratsiooni.	Arendusosa kond

NA-113	Nõuded lähetkoodile ja paigaldamisele	Kui kokku pole lepitud teisiti, siis Python rakenduse kood peab olema kirjutatud vastavalt "Style Guide for Python Code " dokumendile.	http://www.python.org/dev/peps/pep-0008/	Arendusosakond
NA-114	Nõuded lähetkoodile ja paigaldamisele	Kui kokku pole lepitud teisiti, siis .NET rakenduse kood peab olema kirjutatud vastavalt "NET Framework Developer's Guide - Design Guidelines for Developing Class Libraries".	http://msdn.microsoft.com/en-us/library/ms229042.aspx. Valideerimiseks kasutatakse 'StyleCop' vaikimisi konfiguratsiooni.	Arendusosakond
NA-115	Nõuded lähetkoodile	JAVA koodi valideerimiseks kasutatakse validaatorit.	Näiteks PMD (http://pmd.sourceforge.net), DocCheck (http://java.sun.com/j2se/javadoc/doccheck/) või muud võrreldavat kokkulepitud validaatorit.	Arendusosakond
NA-116	Nõuded lähetkoodile	.NET koodi valideerimiseks kasutatakse validaatorit.	Näiteks FxCop (http://msdn.microsoft.com/en-us/library/bb429476.aspx) või muud võrreldavat kokkulepitud validaatorit.	Arendusosakond
NA-117	Nõuded lähetkoodile	Pythoni koodi valideerimiseks kasutatakse validaatorit.	Näiteks Pychecker (http://pychecker.sourceforge.net/) või muud võrreldavat kokkulepitud validaatorit.	Arendusosakond
NA-118	Nõuded lähetkoodile	Kasutuses mitteolev kood tuleb rakenduse lähtekoodist kõrvaldada.		Arendusosakond
NA-119	Nõuded lähetkoodile	Andmebaasi tabelid ja väljad ning muu kood (stored procid, funktsioonid, triggerid, viewd, user defined data types ja sequencid) peab olema kommenteeritud rakenduse koodiga samadel alustel.		Arendusosakond koos infrastruktuuride osakonnaga
NA-120	Nõuded lähetkoodile	Lähtekoodis defineeritud muutujate, klasside/tabelite, meetodite jm. nimed peavad lahenduse kõigis kihtides (rakenduse enda kood, andmebaasjne) olema eesti keelsed.	Mitte Dossier vaid Toimik, mitte Person vaid Isik. NB! Nõuet ei arvestata arendustarkvara poolt automaatselt genereeritavate koodilõikude puhul, mida ei ole vaja tõlkida. Samuti ei rakendata nõuet kolmandate osapoolte poolt toodetud lähtekoodile.	Arendusosakond
NA-121	Andmekvaliteet ja standardid	Aadressiandmete sisestamisel, kuvamisel ja hoidmisel tuleb lähtuda määrusest "Aadressiandmete süsteem".	Liidestatakse maa-ameti X-tee teenusega või RIK sisemise vastava Maa-ameti andmeid vahendava süsteemiga.	Haldur

NA-122	Andmekvaliteet ja standardid	Andmete sisestamisel (ka läbi masin-masin liideste või veebiteenuste) peab rakendus alati andmed valideerime. Sobimatuid andmeid ei tohi olla võimalik sisestada.	Muu hulgas peab kontrollima, kas sisestatav väärtus vastab välja tüübile ja/või etteantud valikväärtustele. Numbriväljale tohib sisestada vaid numbreid, kuupäeva väljale kuupäeva, elektronposti aadressi vilajale elektronposti aadressi, valikväärtuste korral vaid lubatud valikväärtused jne. Kontrollima peab sisendi suurust. Olukorras, kus veebirakendus peab töötlema potentsiaalselt ohtlikke andmeid (nt tähemärke, millel on rakendatava interpretaatorprogrammi jaoks tähendus) ja filtreerimisfunktsiooni ei saa seega kasutada, tuleb need andmed ära maskeerida, st muuta nende kuvamisvormingut. Sisendi kontrolli ebaõnnestumise korral tuleb peatada sisendi kasutamine ja kasutajat sellest teavitada.	Haldur
NA-123	Andmekvaliteet ja standardid	Iga transaktsiooni juures tuleb veenduda, et kasutajal on õigus neid vaadata või muuta (isiku õiguste, mitte rolli õiguste kontroll)		
NA-124	Andmekvaliteet ja standardid	Tegevusalade andmete sisestamisel, kuvamisel ja hoidmisel tuleb lähtuda Vabariigi Valitsuse 10. Jaanuari 2008. a määrusest nr 11 "Klassifikaatorite süsteem" ja kasutada EMTAK infosüsteemis kehtivat klassifikaatorit.	Liidestatakse RIK EMTAK infosüsteemi teenusega.	Arendusosakond
NA-125	Andmekvaliteet ja standardid	Kasutaja poolt sisestatud andmed tuleb enne välja kuvamist filtreerida.	Kasutada tuleks võimalusel Blacklistingu asemel whitelistingut.	Arendusosakond
NA-126	Andmekvaliteet ja standardid	Kui rakendusel tekib päringu töötlemisel tehniline viga, siis peab vastama süsteemi-infot mittesisaldava veateatega.	Näiteks: "Tekkis tehniline viga. Päringu ID: XXXXX".	
NA-127	Dokumentatsioon	Kogu rakenduse dokumentatsioon peab olema kirjutatud eesti keeles.	Erandiks võivad olla tellijaga kokkuleppel kolmanda osapoole komponentide (mis pole kirjutatud tellija jaoks) dokumentatsioon.	
NA-128	Dokumentatsioon	Rakenduse dokumentatsioon peab vastama RIK dokumentatsiooniplaani nõuetele.		
NA-129	Dokumentatsioon	Iga uue versiooniga peab alati välja tooma versiooni muudatuse kirjeldused (release notes).	Release notes peab kajastama kõiki muudatusi eelmise ja uue versiooni vahel.	Haldur koos infrastruktuuride osakonnaga

NA-130	Versioonihaldus	Kõik rakenduse testimiseks, koolituseks või implementeerimiseks üle antavad tarkvarapaketid peavad olema versioneeritud vastavalt dokumendile RIK Arendamise tavad ja töökorraldus. Kasutama peab RIK-i koodihoidlat.	Arendajale antakse selleks õigused RIK-i koodihoidlas, kus ta peab hoidma oma PMA versioone.	Arendusosakond
NA-131	Versioonihaldus	Arendaja peab veenduma, et teeb muudatusi aktuaalsesse koodi.	Paralleelse arendamise puhul võetakse igal hommikul RIK koodihoidlast viimane seis koodist.	Arendusosakond
NA-132	Versioonihaldus	Kõik rakenduste tellijale lepingujärgsete üleantavate versioonide lähtekoodid peavad olema varustatud arendaja esindaja digiallkirjaga.	Ka tagant järgi peab olema 100% kindel, et üle anti õige arendaja signeeritud, mitte kolmanda osapoole poolt kompromiteeritud versioon.	Tellijapoolne projektijuht
NA-133	Versioonihaldus	Nii arendamisel kui ka hoolduslepingute korral kasutatakse RIK vigadehalduse keskkonda.	Kui ei ole tellijaga kokku lepitud teisiti.	Haldur
NA-134	Versioonihaldus	Kui veebirakenduses või veebilehel on linke, mida kasutajad näevad või millele nad saavad viidata, peavad need olema puhtad lingid.	Puhas link on inimloetav, tähendust omav, paraja pikkusega, tekstiline (erandina lubatud numbrid ja märgid „/“, „.“, „-“ ja „_“) ja ajas püsiv. Veebisaidi igal kuval peab olema unikaalne link.	Haldur
NA-135	Paigalduspaketi kooste	Kooste kirjelduste alusel valmiv paigalduspakett tohib sisaldada ainult minimaalse rakenduse käitamiseks vajamineva failikomplekti.	Näiteks: kompileeritavate keelte puhul ei tohi sisaldada lähtekoodi, kui see pole vajalik rakenduse käitamiseks.	Arendusosakond koos infrastruktuuride osakonnaga
NA-136	Paigalduspaketi kooste	Kooste kirjelduste alusel valmivat paigalduspaketti peab olema võimalik liigutada erinevate serverite vahel.	Eelkõige ei tohi tekitada olukorda, kus rakenduse jooksutamiseks uues serveris, tuleb see tingimata just sealsamas kokku kompileerida.	Arendusosakond koos infrastruktuuride osakonnaga
NA-137	Paigalduspaketi kooste	Lähtekoodi kompileerimine peab olema teostatav ka Interneti ühenduse puudumise korral.	Selle nõude täitmise võimaldamiseks on RIK-is kasutusel sisemised tarkvarakomponentide repod.	Arendusosakond
NA-138	Paigalduspaketi kooste	Andmebaasi paigalduse skriptid ei tohi olla kompileeritud.	Administraator peab saama veenduda skriptide sisus.	Infrastruktuuride osakond

Lisad:

Lisa 1 – Staatuslehe nõuded