Kliendirakenduse keskkonnast nõusolekute andmise loogika

Ärivajaduste/probleemi kirjeldus

Hetkel nõuab nõusoleku andmise protsess lõppkasutaja (edaspidi Andmesubjekti) suunamist kliendirakendusest (ettevõtte veebikeskkonnast) Nõusolekuteenuse keskkonda (eesti.ee/nõusolek) ning seejärel tagasi kliendirakenduse keskkonda. Selle raames autenditakse Andmesubjekt kliendirakenduse teenuse kasutamisel kaks korda - esmalt teenusesse endasse sisselogimisel ning seejärel Nõusolekuteenusesse suunamisel (TARA kaudu). Selleks, et tagada lõppkasutajale maksimaalselt mugav kasutajakogemus ja vältida ebamugavat liikumist erinevate keskkondade vahel, tuleks edaspidi võimaldada nõusolekut anda kliendirakenduse keskkonnas.

Lahenduse visioon

Käesolevas peatükis kirjeldatakse Kliendirakenduse keskkonnast nõusoleku andmise loogikat ja ärilist visiooni, mille koostamisel on arvestatud nii Hankija poolt viidatud dokumentatsioonis esitatud põhimõtete kui ka tulevikuperspektiiviga.

Lõppkasutaja mugavuse parendamiseks luuakse võimalus nõusolekuid anda Nõusolekuteenuse väliselt, mille korral nõusoleku andmine toimub ainult Kliendirakenduses. Turvalisuse tagamiseks eeldame, et Andmesubjekt on kliendirakendusse sisse loginud läbi turvalise autentimise meetodi (ID-kaardiga, Mobiil-ID'ga või Smart-ID'ga).

Kliendirakenduse kasutaja (st Andmesubjekt) soovib kasutada Kliendirakenduse teenust, milleks on vajalik Andmesubjekti nõusolek. Kliendirakendus kontrollib kõigepealt läbi Nõusolekuteenuse, kas Andmesubjekt, kelle kohta nõusolekuid küsitakse, on täisealine ja teovõimeline. Andmeid kontrollitakse läbi Rahvastikuregistri. Kui need tingimused ei ole täidetud, tagastab Nõusolekuteenus Kliendirakendusele veateate. Kui Andmesubjekt on täisealine ja teovõimeline, siis jätkatakse kontrolliga, kas Andmesubjektil on teenuse tarbimiseks kõik vajalikud nõusolekud olemas. Selleks kasutatakse juba olemasolevat loogikat, mis on kirjeldatud Nõusolekuteenuse dokumentatsioonis (ver 1.0, leitav GitHub[1]).

[1] https://github.com/e-gov/NT/blob/master/RIA%20n%C3%B5usolekuteenuse%20kasutamine%20ja%20liidestamine%20ver%201.0%20-%2015.09.2021/RIA%20n%C3%B5usolekuteenuse%20kasutamine%20ja%20liidestamine%20ver%201.0%20-%2015.09.2021.md

Kui selgub, et teenuse tarbimiseks on mõni nõusolek puudu (puuduolevateks nõusolekuteks loetakse ka nõusolekuid, mis olid juba varasemalt antud, aga olid aegunud või Andmesubjekti poolt tagasi võetud), pöördub Kliendirakendus Nõusolekuteenuse poole ning pärib nõusolekutaotluse(d) puuduoleva(te) nõusoleku(te) andmiseks. Nõusolekuteenus tagastab küsitud nõusolekutaotluse(d) ning Kliendirakendus kuvab need Andmesubjektile ülevaatamiseks ja allkirjastamiseks, ilma, et kasutaja peaks Kliendirakendusest lahkuma. Riskina saame välja tuua selle, et puudub kontroll selle üle, kuidas või mis kujul Kliendirakendus Nõusolekuteenusest edastatud infot kasutajale kuvab ja seeläbi võib Andmesubjekt anda nõusoleku tekstile (nõusolekutaotlusele), mida Nõusolekuteenus edastanud ei ole.

Kui Andmesubjekt on nõusolekutaotluse(d), st metaandmed ja DigiDoc konteineris oleva nõusoleku pdf faili üle vaadanud, kinnitab Andmesubjekt iga nõusoleku digitaalse allkirjaga. Digitaalne allkiri aitab tagada nõusoleku tõendusväärtuse ja kinnitab, et just see konkreetne Andmesubjekt on nõusoleku andja. Kui aga Andmesubjekt ei nõustu nõusolekut andma, saab ta nõusolekutaotluse tagasi lükata, jättes selle digitaalselt allkirjastamata. Tagasi lükatud nõusolekutaotlus(t)e kohta Nõusolekuteenust ei teavitata. Nõusolekutaotlus(ed) jäävad Nõusolekuteenuses staatusesse "Otsuse ootel", kuniks käivitub vastav taustatöö (vt 3.2.1.1 Taustatöö), mis antud nõusolekutaotluse(d) kustutab.

Kliendirakendus saadab allkirjastatud nõusolekud, kas kõik korraga või ükshaaval Nõusolekuteenusesse. Nõusolekuteenus muudab allkirjastatud nõusolekutaotluse(d) kehtiva(te)ks nõusoleku(te)ks ja omistab neile nõusolekuviited. Kliendirakendus kuvab Andmesubjektile vastavalt Nõusolekuteenusest saadud vastuse põhjal teadet.

Juhul, kui Andmesubjekt lahkub lehelt ilma nõusolekuid kinnitamata, saab ta nõusolekute andmisega jätkata, kui naaseb Kliendirakenduse lehele, kus alustatakse protsessi algusest: tuvastatakse Andmesubjekti puuduoleva(d) nõusoleku(d) ning küsitakse Nõusolekuteenuselt puuduoleva(te) nõusoleku(te) nõusolekutaotlus(ed) Andmesubjektile ülevaatamiseks ja allkirjastamiseks.

Kui andmeedastuses esineb probleeme, siis kõik vigased olukorrad on ära fikseeritud veateadetega, mida Nõusolekuteenus Kliendirakendusele tagastab. Veateadete loogika on esitatud tehnilise visiooni kirjelduses.

Nõusolekute haldamine

Nõusolekute hilisemaks halduseks kuvatakse kõik Kliendirakenduses antud nõusolekud keskkonnas eesti.ee/nousolek. Tegu on olemasoleva keskkonnaga, kuhu sisse logides kuvatakse ülevaade

Andmesubjekti poolt antud nõusolekutest, loobutud nõusolekutest ning andmejälgijast, mis annab ülevaate nõusolekute kasutamisest.

Nõusolekute hilisemat haldamist Kliendirakenduse keskkonnast ei realiseerita. Nõusolekuteenusesse tehtavad päringud kasutajat identifitseeriva infoga (näiteks isikukood) ei taga mitte mingil moel, et antud infoga kasutaja reaalselt ise Kliendirakendust päringu hetkel ka kasutab. Turvariski vältimiseks jääb nõusolekute hilisem haldus ainult läbi eesti.ee/nousolek keskkonna.

Tehnilise visiooni kirjeldus

Käesolevas peatükis on esitatud Kliendirakenduse keskkonnast nõusoleku andmise tehnilise lahenduse visioon, mis hõlmab nii Nõusolekuteenuse API kirjeldust kui ka andmebaasis tehtavaid muudatusi.

API kirjeldus

Nõusolekuteenus pakub REST API päringuid üle X-tee. Selleks, et nõusoleku andmine saaks toimuda Kliendirakenduse keskkonnas, on vajalik juurde lisada kaks täiendavat päringut: „Nõusolekutaotluse küsimise päring“ ja „Allkirjastatud nõusoleku edastamise päring“.

Uutele päringutele rakendub olemasolev Nõusolekuteenuse REST API loogika, kus päringud hakkavad samuti käima üle X-tee.

Allkirjastatud nõusoleku edastamise päring

Päringu abil saab Nõusolekuteenusele edastada allkirjastatud nõusoleku(id).

Kasutab: Kliendirakendus
API URL: https://cons-consent-01.dev.riaint.ee/api/consent/third-party/container
Päringu meetod: POST

Päringu sisend

Päringu sisendiks antakse nõusoleku(te) UUID ja digitaalselt allkirjastatud DigiDoc konteiner(id). Sisend koosneb massiivist, mis sisaldab üks kuni mitu allkirjastatud nõusolekut. Üks nõusolek koosneb nõusoleku UUID väärtusest ja allkirjastatud digikonteinerist, milles nõusoleku fail pdf kujul.

Päring (Json):


```
[{
        "consentConfirmReference": "7bf5904a-bce3-483f-99c2-527937b032b7",
        "file": "0gaXBzdW0gZG9sb3Igc2l0IGFtZXQsIGNvbnNlY3RldHVyIGFkaXBpc2Npbmcg"
}, {
        "consentConfirmReference": "f16904d0-6f9c-44b4-96a6-ae2106ab326b",
        "file": " yaWNpZXMgc2NlbGVyaXNxdWUuIE5hbSB2YXJpdXMgbW9sZXN0aWUgbmlzaS"
}]
```


Parameeter	On kohustuslik?	Andmetüüp	Kirjeldus
consentConfirmReference	Jah	String	Otsuse ootel nõusoleku UUID
file	jah	String	Allkirjastatud nõusolek (DigiDoc konteiner ASICE formaadis) Stringi sees base64 kodeeritud fail.

Päringu vastus

Päringu vastuseks on massiiv, mis sisaldab iga nõusoleku kohta vastust andmete töötlemise õnnestumise/mitteõnnestumise kohta. Massiiv koosneb otsuse ootel nõusoleku UUID väärtusest, staatusest (Status) ning errorCode väärtusest, kui andmete töötlemine ebaõnnestub.

Vastus (Json):


```
[{
        "consentConfirmReference": "7bf5904a-bce3-483f-99c2-527937b032b7",
        "status": "OK"
}, {
        "consentConfirmReference": "f16904d0-6f9c-44b4-96a6-ae2106ab326b",
        "status": "ERROR",
        "errorCode": "CONSENT_NOT_FOUND"
}]
```

Parameeter	On kohustuslik?	Andmetüüp	Kirjeldus
consentConfirmReference	Jah	String	Otsuse ootel nõusoleku UUID
status	Jah	String	· Kui andmete töötlemine õnnestub, tagastatakse staatuseks „OK“; · Kui andmete töötlemine ei õnnestunud, tagastatakse staatuseks „ERROR“, koos vastav errorCode väärtusega.
errorCode	Ei	String	· „HTTP_NOT_FOUND“ - X-road client ei ole sama, mis nõusolekuga seotud teenusedeklaratsioonis; · CONSENT_VALIDATE_INVALID – sisendis antud nõusoleku andmed ei ühti andmebaasis oleva nõusolekuga (vt „Päringu andmete kontrollimine ja salvestamise loogika). · CONSENT_NOT_FOUND – sisendis antud UUID ei leidu andmebaasist.

Päringu andmete kontrollimine ning salvestamise loogika

Nõusolekuteenus töötleb sisse tulnud päringut. Päringu töötlemise käigus võrreldakse päringuga tulnud andmeid andmebaasis olevaga, kus kontrollitakse:

Kas päringu teinud X-tee klient (x-road client) ühtib andmebaasis oleva nõusolekuga seotud teenusedeklaratsioonis olevaga.

Kas UUID järgi leitud andmebaasi kirjes ühtivad kontroll väljad nõusoleku infoga.

Kas allkirjastatud DigiDoc konteiner ja allkiri on valiidne.

Kas DigiDoc konteineris olev pdf räsi ühtib andmebaasi konteineris oleva pdf räsiga.

Kas allkiri on antud viimase tunni aja jooksul (ajaperiood reguleeritav süsteemse parameetriga).

Kas allkirjas olevad isiku andmed (isikukood, eesnimi, perekonnanimi) ühtivad andmebaasis oleva infoga.

Kui andmete kontrollid saavad positiivse vastuse („status“:„OK“), salvestatakse andmed andmebaasi „Consent“ järgnevatesse tabelitesse: CONSENT, CONSENT_SNAPSHOT, FILE. Tabelis „FILE“

olev allkirjastamata DigiDoc konteiner asendatakse päringust tulnud allkirjastatud DigiDoc konteineriga.

Vea korral tagastatakse staatus koos veakoodiga (vt Päringu vastus).

Nõusolekutaotluse küsimise päring

Päringu abil saab Klientrakendus küsida Nõusolekuteenuselt nõusolekutaotluse(id) puuduva(te) nõusoleku(te) andmiseks.

Kasutab: Kliendirakendus

API URL: https://cons-consent-01.dev.riaint.ee/api/consent/third-party

Päringu käsu näide (curl):

```
curl -k \
  -H "accept: application/json" \
  -H "Content-Type: application/json" \
  -H "X-Road-Client: ee-dev/GOV/70006317/consent" \
"https://<turvaserveri-aadress>/r1/ee-dev/GOV/70006317/consent/consent-stage/api/consent/third-party"
\ -d "{
\"idCode\": \"60001019906\", \
\"purposeDeclarationBusinessIdentifiers\": [\"EesmärgideklaratsiooniID\", \"ED_KAKS\", \"ED_KOLM\"], \
\"firstName": "eesnimi\", \
\"lastName": "perenimi\" \
}"
```

Päringu meetod: POST

Päringu sisend

Päringu sisendiks antakse Andmesubjekti isikukood, ees-ja perekonnanimi ning eesmärgideklaratsiooni identifikaator(id).

Päring (Json):

```
{
        "idCode": "60001019906",
        "firstName": "Jaan",
        "lastName": "Tamm",
        "purposeDeclarationBusinessIdentifiers": ["ED_KAKS", "ED_KOLM"]
}
```

Parameeter	On kohustuslik?	Andmetüüp	Kirjeldus
idCode	Jah	String	Andmesubjekti isikukood
purposeDeclarationBusinessIdentifiers	Jah	Array of String	Eesmärgideklaratsiooni identifikaator. Saab olla mitu
firstName	Jah	String	Andmesubjekti eesnimi
lastName	Jah	String	Andmesubjekti perekonnanimi

Päringu vastus

Päringu vastuseks antakse nõusolekutaotlus(t)e andmekomplekt JSON kujul. Vastus koosneb massiivist, mis sisaldab üks kuni mitu nõusolekutaotlust. Üks nõusolekutaotlus koosneb nõusolekutaotluse metaandmetest ja allkirjastamata digikonteinerist, milles sisaldub nõusolekutaotluse fail pdf kujul.

Vastus (Json):


```
[{
                "consentConfirmReference": "7bf5904a-bce3-483f-99c2-527937b032b7",
                "idCode": "60001019906",
                "firstName": "Jaan",
                "lastName": "Tamm",
                "clientName": "Health Startup OÜ",
                "clientRegistryCode": "12819685",
                "clientService": "Immu",
                "purposeDeclarationDescription":  " Kui lubate Vaktsiinide
infosüsteemil enda
immuniseerimisandmed Health Startup OÜ-le edastada, võimaldab see teile pakkuda
vaktsineerimiste nõustamise ja meeldetuletuse teenust Immu.
                "serviceDeclarationName": "Tervise_immuniseerimisandmed ",
                "serviceDeclarationDescription": "Immuniseerimistega seotud andmed:
```

```
haigus mille vastu immuniseeriti,

immuniseerimise kuupäev,

immunpreparaadi ATC kood ja toimeaine(te) nimetus(ed).",

"dataProviderName": " Vaktsiinide Infosüsteem ",

                "dataControllerName": " Sotsiaalministeerium ",

                "dataControllerRegistryCode": "70001952",

                "dataProcessorName": " Tervise Infosüsteemide Amet ",

                "dataProcessorRegistryCode": "70006317",

                "validFrom": "01.01.2022",

                "validTo": "01.01.2024",

                "file": wMzczMiAwMDAwMCBuIAowMDAwMDE4MzY1IDAwMDAwIG4gCjAwMDAwM

Tg0NDcgMDAwMDAgbiAKMDAwMDAxODczOCAwMDAwMCBuIAowMDAwMDE5MTE1IDAwMIG4gCjAwMDAwMTkxNzgg
MDAwMDAgbiAKMDAwMDAxOTI4MiAwMDAwMCBuIAow"

}, {

                "consentConfirmReference": "f16904d0-6f9c-44b4-96a6-ae2106ab326b",

                "idCode": "60001019906",

                "firstName": "Jaan",

                "lastName": "Tamm",

                "clientName": " Health Startup OÜ ",

                "clientRegistryCode": "12819685",

                "clientService": "koroonapassi kontroll",

"purposeDeclarationDescription": " Kui lubate Tervise Infosüsteemil edastada Health
Startup OÜ-le oma COVID-19 immuniseerimisega seotud andmed, siis saab Health Startup
AS pakkuda teile automaatset koroonapassi kontrolli teenust. ",

                "serviceDeclarationName": "immuandmed",

                "serviceDeclarationDescription": "Immuniseerimistega seotud andmed:

immuniseerimise kuupäev,
immuunpreparaat",

                "dataProviderName": "Tervise Infosüsteem",

                "dataControllerName": "Sotsiaalministeerium",

                "dataControllerRegistryCode": "70001952",
```

```
                "dataProcessorName": "Terviseamet"

                "dataProcessorRegistryCode": "70008799",

                "validFrom": "01.01.2022",

                "validTo": "01.01.2023",

"file": "wQMzczMiAwMDAwMCBuIAowMDAwMDE4MzY1IDAwMDAwIG4gCjAwMDAwM
Tg0NDcgMDAwMDAgbiAKMDAwMDAxODczOCAwMDAwMCBuIAowMDAwMDE5MTE1IDAwMDAwIG4gCjAwMDAwMTkxN
zggMDAwMDAgbijAKMDAwMDAxOTI4MiAwMDAwMCBuI"

}]
```


Parameeter	**On kohustuslik?**	**Andmetüüp**	**Kirjeldus**
consentConfirmReference	Jah	String	Otsuse ootel nõusoleku UUID
idCode	Jah	String	Isikukood
firstName	Jah	String	Eesnimi
lastName	Jah	String	Perekonnanimi
clientName	Jah	String	Osapoole nimi (e Kliendirakendus), kellele nõusoleku alusel andmed edastatakse
clientRegistryCode	Jah	String	Osapoole registrikood, kellele nõusoleku alusel andmed esitatakse
clientService	Jah	String	Andmete saaja pakutav teenus
purposeDeclarationDescription	Jah	String	Eesmärgideklaratsiooni kirjeldus (Andmete kasutamise eesmärk).
serviceDeclarationName	Jah	String	Teenusedeklaratsiooni nimi
serviceDeclarationDescription	Jah	String	Andmete edastaja andmete kirjeldus/teenuse andmekoosseisu kirjeldus.
dataProviderName	Jah	String	Andmekogu/ infosüsteemi nimi
dataControllerName	Jah	String	Andmete edastaja vastutav töötleja
dataControllerRegistryCode	Jah	String	Andmete edastaja vastutava töötleja registrikood

dataProcessorName	Jah	String	Andmete edastaja volitatud töötleja
dataProcessorRegistryCode	Jah	String	Andmete edastaja volitatud töötleja registrikood
validFrom	Jah	String	Nõusoleku kehtivus: alates Timestamp sisuga string Nt 01.01.2022
validTo	Jah	String	Nõusoleku kehtivus: kuni Timestamp sisuga string Nt 01.01.2023
file	jah	String	Allkirjastamata konteiner (Asice) nõusolekutaotluse pdf failiga. Stringi sees base64 kodeeritud fail.

Andmete pärimise ja salvestamise loogika

Nõusolekuteenus töötleb sisse tulnud päringut ning genereerib sisendis esitatud isikukoodi ja eesmärgideklaratsiooni kombinatsiooni baasil nõusolekutaotluse andmekomplekti, mis pannakse kokku kolmes erinevas andmebaasis (Purpose declaration, Service declaration ja Consent) oleva info põhjal. Kui sisendis on mitu eesmärgideklaratsiooni, siis iga eesmägideklaratsiooni kohta genereeritakse eraldi andmekomplekt ehk nõusolekutaotlus. Igale nõusolekutaotlusele (otsuse ootel nõusolekule) omistatakse unikaalne UUID, mis salvestatakse andmebaasi „Consent“ tabelisse „CONSENT“ väljale „CONSENT_GROUP_REFERENCE“.

Nõusolekutaotluse andmekomplekt sisaldab nõusolekutaotluse metaandmeid ja süsteemi poolt genereeritud DigiDoc konteinerit, milles on nõusoleku andmetest kokku pandud fail pdf kujul. Nõusolekutaotluse andmekomplekti koostamise käigus toimub ka nõusolekutaotluse andmete sh DigiDoc faili salvestamine „Consent“ andmebaasi tabelitesse „CONSENT“, „FILE“ ja „CONSENT_FILE“.

Veahaldus

Käesolevas peatükis on kirjeldatud nõusolekutaotluse küsimise päringu poolt tagastatavad vastused päringu vea korral. Tegu on Nõusolekuteenuses kasutuses olevate veakoodidega, mida kasutatakse ka käesoleva (proovi)töö raames kirjeldatud päringus.

Vea võti	Veakood ja staatus	Vea kirjeldus
error.validation	VALIDATION (400)	Validatsiooni üldised veateated (kohustuslikud väljad määramata, isikukood <>11 märki, mittenumbriline)
error.business.requested-consents-not-related-to-any-declarations	REQUESTED_CONSENTS_NOT_RELATED_TO_ANY_DECLARATIONS (404)	Kehtiva eesmärgideklaratsiooni ja alamsüsteemi kombinatsiooni ei leitud kõikide küsitud nõusolekute puhul
error.business.id-code-invalid	ID_CODE_INVALID (400)	Isikukood ei vasta standardile
error.business.requested-consents-related-to-invalid-declarations	REQUESTED_CONSENTS_RELATED_TO_INVALID_DECLARATIONS (500)	Küsitud nõusolekud on seotud kehtetute eesmärgideklaratsioonidega. Küsitud äriidentifikaatorid, mis on seotud kehtetute eesmärgideklaratsioonidega, eesmärgideklaratsiooni mikroteenuse andmebaasis on loetletud vea kirjelduses
error.business.all-requested-consents-have-already-been-approved	ALL_REQUESTED_CONSENTS_HAVE_ALREADY_BEEN_APPROVED (500)	Nõusolekute mitmekordsel küsimisel juhul, kui kõik leitud nõusolekud on staatuses APPROVED
error.business.data-subject-error	DATA_SUBJECT_ERROR (500)	Isikukoodi järgi on isik alaealine ja või teovõimetu