CYBERNETICA

Euroopa Liit
Euroopa
Regionaalarengu Fond

Eesti
tuleviku heaks

Tõend kui platvorm

Näidisrakenduse kirjeldus

Dok: D-25-1
12.05.2022

Projektijuhid: Katrin Kivi (Riigi Infosüstemi Amet)
Andrei Kargin (Riigi Infosüstemi Amet)
Kaija Kirch (Cybernetica)
Liis Peets (Cybernetica)

Autorid: Alisa Pankova, PhD (Cybernetica)
Peeter Laud, PhD (Cybernetica)
Aivo Kalu, PhD (Cybernetica)
Rauni Lillemets, PhD (Cybernetica)
Maria Toomsalu (Cybernetica)
Martin Johannes Liba (Cybernetica)
Aleksander Kamenik (Cybernetica)

Riigi Infosüsteemi Amet, Pärnu maantee 139a, 15169 Tallinn, Eesti.

Email: ria@ria.ee, Web: https://www.ria.ee, Telefon: +372 663 0200.

Cybernetica AS, Mäealuse 2/1, 12618 Tallinn, Eesti.

E-mail: info@cyber.ee, Web: https://www.cyber.ee, Telefon: +372 639 7991.

Sisukord

1. Sissejuhatus

Käesolev dokumentatsioon kirjeldab "Tõend kui platvorm" projekti raames loodud näidisrakendust, millega demonstreeritakse analüüsidokumendis kirjeldatud tehnilisi võimalusi olemasolevate tõendite ja isikut tõendavate dokumentide nutiseadmete kasutamise kontekstis.

Dokumentatsioon on koostatud Riigi Infosüsteemi Ameti tellimusel Riigis puudub ühtne lahendus, millega isik saaks oma õigusi ja andmeid tõendada, sõltumata keskkonnast ning teenuseosutaja võimekusest saada riigilt isiku kohta andmeid.

1.1. Näidisrakenduse olemus

Tõend kui platvorm projekti raames loodud kontrollimise ja digikukru näidisrakendus põhinevad projekti analüüsidokumendis kirjeldatud mDL formaadil.

Rakenduste tegemisel on aluseks võetud avaliku lähtekoodiga Google poolt loodud näidisrakendused repositooriumist *mdl_ref_apps* [1] . Näidistõenditena kasutatakse harrastuskalapüügiõigust tõendavat tõendit ja kahte ID-kaarti. Kontrollrakenduse abil saab õigust/privileegi kontrollida ühe tõendi (näiteks ID-kaart) andmeid sisaldava tõendi esituse põhjal või mitme erineva tõendi andmeid sisaldava seostatud tõendi esituse põhjal. Seostatus tähendab, et erinevad tõendid on omavahel lingitud ühise identifikaatori abil. Näidisrakenduse tõendite puhul on selleks isikukood ning seostatud tõendi esitus koosneb andmetest harrastuspüügiõigust tõendavalt tõendilt ja näofotost ID-kaardilt.

Tõendi kontroll kahe seadme vahel töötab mDL formaadis kirjeldatud vallasrežiimis. Lisaks tõendi esituse kontrollile demonstreerib digikukru näidisrakendus, kuidas tõendit digikukrusse lisatakse, kustutatakse ja kuidas tõendi omanik saab tõendi väljastamisega seotud infot vaadata. Need kolm funktsionaalsust (lisamine, kustutamine, info vaatamine) pole kirjeldatud mDL ISO-18013-5 standardis ja seega ei põhine mDL formaadil. Tõendi väljastamiseks digikukrusse on olemas ka piiratud funktsionaalsusega serverrakendus.

Järgnevalt on kirjeldatud näidisrakenduse funktsionaalsust kirjeldavad kasutusmallid. Pärast seda on defineeritud näidistõendite (ID-kaart ja harrastuskalapüügiõiguse tõend) andmeelemendid ja näidisandmete komplektid.

1.2. Mõisted

- **Tõend** on kinnitus või dokument, mis vastavalt oma tüübile kinnitab **tõendi subjekti** kohta mingeid väiteid. Tõend võib olla nii füüsiline (paber/plastkaart) kui ka elektrooniline (e-tõend). Tõendile on määratud protsessi nõuetest lähtuv kehtivusaeg. Mõisteid "tõend", "e-tõend", "elektrooniline tõend" on selles dokumendis elektroonilise tõendi sünonüümid.
- **Tõendi omanik** on füüsiline isik, kellele tõend on välja antud.
- **Kasutaja** on füüsiline isik. Seda mõistet kasutame näiteks siis, kui füüsiline isik pole veel tõendit kätte saanud, või pole veel tõestanud, et ta on tõendi subjekt või tõendi omanik.
- **Tõendi esitus** on ühe või mitme tõendi andmetest koosnev kogum, mis kinnitab tõendi(te) omaniku privileegi või õigust. Näiteks, vaktsiinipass koos isikut tõendava dokumendiga annab isikule õiguse kohvikus kohapeal süüa. Mitmest tõendist koosnev esitus seostatakse tõendites oleva ühise identifikaatori abil.

- **Digikukru rakendus** (või lihtsalt **digikukkur**) on tõendi omaniku (nuti)seadmesse paigaldatud rakendus, mis lubab tõendi omanikul esitada **kontrollijale** oma tõendi(te) andmetest koosneva tõendi esituse.
- **Väljaandja** on asutus, mis on volitatud koostama tõendeid. Väljaandja vastutab tõendi andmete korrektsuse eest.
- **Kontrollija** on osapool, kes tahab veenduda, et kasutajal on olemas privileeg või õigus. Tehniliselt saab kontrollija kasutaja käest tõendi esituse, mis sisaldab andmeid, mida kontrollitakse.
- **Kontrollimine** on protseduur, mille käigus kontrollija veendub, et kasutajal on olemas privileeg või õigus. Kontrollimine koosneb **verifitseerimisest** ja **valideerimisest**.
- **Verifitseerimine**: esitatud andmed on terviklikud ja autentsed (ei ole võltsitud), tõend on signeeritud väljaandja(te) poolt ning tõend on ajaliselt kehtiv. Verifitseerimist saab tavaliselt teostada automaatselt ning see protseduur ei sõltu konkreetsest tõendist (kas tegemist on näiteks juhiloaga või kalastustõendiga). Andmete ehtsust tõendavad krüptograafilised signatuurid. Verifitseerimist teostab **kontrollimise rakendus**, mis asub **kontrollimise seadmes**.
- **Valideerimine**: esitatud andmed annavad esitajale teatud privileegi/õigust. Tüüpiliselt hõlmab see veendumist, et tõendi esitatav kasutaja on tõendi omanik (isikusamasuse kontroll) ning et tõend on kehtiv. Kehtivuse kontroll jääb valideerimise alla, sest see sõltub äriloogikast. Näiteks, teatud juhul võib ka eile kehtivuse kaotanud tõend siiski olla õiguse tõendamiseks piisav. Valideerimist teostab kontrollija kasutades kontrollimise rakenduse poolt kuvatud andmeid ja verifitseerimise tulemust (kui tegemist on tõendi füüsilise esitamisega) või teostades valideerimist mõnel muul viisil (kui tegemist on e-teenusega).
- **Autentimisvõti**: võtmed, mis väljastatakse tähtajaliselt serveri poolt konkreetse tõendi väljade terviklikkuse tagamiseks. Võimaldab tõendite andmete osalist jagamist.

1.3. Lühendid

- BLE - *Bluetooth Low Energy*
- mDL - *Mobile Driving Licence*
- QR - *Quick Response*

2. Kasutusmallid

2.1. Kasutusmall 01 - Kontrolli õigust tõendi esituse abil.

Tegijad

- Kontrollija
- Kontrollrakendus
- Tõendi omanik
- Digikukkur

Eeltingimused

Tõendi omaniku seadmes on käivitatud digikukru rakendus, mis sisaldab õiguse/privileegi kontrolliks vajalikke tõendit/tõendeid. Kontrollija seadmes on käivitatud kontrollrakendus.

Õnnestumise peastsenaarium

1. Kontrollija valib kontrollrakenduses kontrolliks vajaliku tõendi esituse valiku. See võib olla ühe tõendi andmetest koosnev tõendi esitus või mitme tõendi andmetest koosnev seostatud tõendi esitus.
2. Kontrollrakendus loob digikukru rakendusega seadmetevahelise ühenduse. [Kasutusmall 02 - Loo seadmetevaheline ühendus.]
3. Kontrollrakendus saadab tõendi esituse päringu digikukru rakendusele.
4. Digikukru rakendus kuvab tõendi(te) ja andmeväljade nimetused, mida kontrollrakendus pärib ja küsib omaniku nõusolekut nende saatmiseks.
5. Tõendi omanik annab digikukru rakenduses loa küsitud andmete saatmiseks kontrollrakendusele.
6. Digikukru rakendus koostab vastava tõendi esituse ja saadab selle kontrollrakendusele ning kuvab ühenduse staatuse, saadetud tõendite nimed ning serveeritud päringute arvu.
7. Kontrollrakendus verifitseerib saadud tõendi esituse.
8. Kontrollrakendus kuvab tõendi esituse kontrollijale järgnevad detailid:
    - Saadud tõendite arv.
    - Tõendi esituse saatja seadme aadress.
    - Info tõendi esituse seostamise verifitseerimise kohta. (Seda infot kuvatakse ainult mitme tõendi andmetest koosneva seostatud tõendi esituse puhul.)
    - Tõendi tüüp (*Doctype*). (Kui tõendi esitus sisaldab andmeid erinevatelt tõenditelt siis esineb mitmel korral)
        - Tõendi väljandja allkirjastamise võtme verifitseerimise info. (Kontrollija näidisrakenduses verifitseerimine ebaõnnestub, sest väljaandja signatuuris pole kasutatud korrektset allkirjastamise võtit)
        - Väljaandja antud tõendi signatuuri verifitseerimise info.

        - Digikukru seadme/rakenduse antud tõendi signatuuri verifitseerimise info.
        - Tõendi nimeruum(id) (*namespace*). (Kui tõendi esitus sisaldab andmeid erinevatest nimeruumidest siis esineb mitmel korral)
            - Nimeruumis sisalduvate andmeelementide väärtused ja nende verifitseerimise info.
9. Kontrollija valideerib õiguse/privileegi kehtivuse, vaadates kuvatavat tõendi esitust ja verifitseerimise tulemuste infot.
10. Kontrollija informeerib tõendi omanikku kontrolli tulemusest.

Laiendid (Stsenaariumid, mis kirjeldavad lahknevusi peastsenaariumist ning võivad olla õnnestumised või nurjumised.)

- 2a. Digikukru rakendus on varasemalt kontrollrakendusega tõendi esitust vahetanud ja selle käigus on seniajani toimiv seadmetevaheline ühendus loodud.
    - 2.a.1 Kasutusmall jätkub sammust 3.
- 5a. Tõendi omanik keeldub küsitud andmeid jagamast.
    - 5.a.1 Digikukru rakenduse katkestab seadmetevahelise ühenduse.
    - 5.a.2 Kasutusmall katkeb
- 6a. Tõendi omanik sulgeb digikukru rakenduses seadmetevahelise ühenduse pärast tõendi esituse saatmist.
    - 6.a.1 Digikukru rakenduse katkestab seadmetevahelise ühenduse.
    - 6.a.2 Kasutusmall jätkub sammust 7.
- 8a. Mitmest tõendist koosneva seostatud tõendi esituse verifitseerimine ebaõnnestub, tagastati vaid üks tõend.
    - 8.a.1 Kontrollrakendus kuvab "info tõendi esituse seostamise verifitseerimise" all teate, et tagastati andmed vaid ühelt tõendilt ja seostamine ebaõnnestus.
    - 8.a.2 Kasutusmall jätkub sammust 9.
- 8b. Mitmest tõendist koosneva seostatud tõendi esituse verifitseerimine ebaõnnestub, kuna tagastatud tõendite seostatavad identifikaatorid ei ühti.
    - 8.b.1 Kontrollrakendus kuvab "info tõendi esituse seostamise verifitseerimise" all teate, et seostamine ebaõnnestus, kuna identifikaatorid ei ühti.
    - 8.b.2 Kasutusmall jätkub sammust 9.
- (8-9)a Kontrollija soovib teha uue tõendi esituse päringu.
    - (8-9).a.1. Kasutusmall jätkub sammust 1.
- (8-9)b Kontrollija sulgeb kontrollrakenduses seadmetevahelise ühenduse.
    - Kontrollrakendus katkestab seadmetevahelise ühenduse.
    - Kasutusmall jätkub järgmisest sammust.

Garantii

Kontrollija on saanud teada õiguse/privileegi kehtivuse kontrollides ühe tõendi andmetest koosnevat tõendi esitust või mitme tõendi andmetest koosnevat seostatud tõendi esitust.

2.2. Kasutusmall 02 - Loo seadmetevaheline ühendus. (QR koodi põhjal)

Tegijad

- Kontrollija
- Kontrollrakendus
- Tõendi omanik
- Digikukru rakendus ehk digikukkur

Eeltingimused

Kontrollija on kontrollrakenduses valinud ühe tõendi andmetest koosneva tõendi esituse või mitme erineva tõendi andmetest koosneva seostatud tõendi esituse, mida pärida digikukru rakenduselt.

Õnnestumise peastsenaarium

1. Kontrollrakendus kuvab kaameravaate QR koodi skaneerimiseks.
2. Kontrollija laseb tõendi omanikul seadmete kaasamiseks esitada digikukru rakenduses QR kood.
3. Tõendi omanik valib digikukru rakenduses tõendi esitamise.
4. Digikukru rakendus kuvab QR koodi seadmete kaasamiseks.
5. Kontrollija suunab kontrollrakenduses kaamera digikukrus kuvatava QR koodi suunas.
6. Kontrollrakendus skanneerib kaamera abil digikukrus kuvatavat QR koodi.
7. Kontrollija valib andmevahetuseks kasutatava BLE meetodi.
8. Kontrollrakendus ja digikukru rakenduse seadmed loovad QR koodi abil vahendatud andmete põhjal BLE ühenduse.

Laiendid (Stsenaariumid, mis kirjeldavad lahknevusi peastsenaariumist ning võivad olla õnnestumised või nurjumised.)

- 1a. Kontrollija katkestab seadmetevahelise ühenduse loomise kontrollrakenduses.
  - 1.a.1 Kasutusmall katkeb.
- 4a. Tõendi omanik katkestab seadmetevahelise ühenduse loomise digikukru rakenduses.
  - 4.a.1 Kasutusmall katkeb.
- 5a. Kontrollija katkestab seadmetevahelise ühenduse loomise kontrollrakenduses.
  - 5.a.1 Kasutusmall katkeb.
- 7a. Kontrollija katkestab seadmetevahelise ühenduse loomise kontrollrakenduses.
  - 7.a.1 Kasutusmall katkeb.

Garantii

Kontrollrakenduse ja digikukru rakenduse seadmete vahel on ühendus loodud.

2.3. Kasutusmall 03 - Väljasta tõend

Tegijad

- Serverrakendus
- Kasutaja
- Digikukru rakendus

Eeltingimused

Serverrakenduses on tõend valmis tarnimiseks.

Õnnestumise peastsenaarium

1. Kasutaja algatab digikukru rakenduses digitaalse tõendi digikukrusse tarnimise protsessi.
2. Digikukru rakendus kuvab serveri URL ja tõendite tarnekoodi sisestamise väljad.
3. Kasutaja täidab rakenduses väljad ja jätkab tõendi tarnimisega.
4. Digikukru rakendus teeb päringu serverrakendusele.
5. Serverrakendus vastab päringule, tagastades *challenge*, mille digikukru rakendus peab allkirjastama.
6. Digikukru rakendus loob uue *self-signed* sertifikaadi ja allkirjastab vastava võtmega serveripoolse *challenge'i*.
7. Digikukru rakendus edastab allkirjastatud *challenge'i* ja *self-signed* sertifikaadi ahela serverrakendusele.
8. Serverrakendus verifitseerib *self-signed* sertifikaadid. (Näidisrakenduses tehakse minimaalselt verifitseerimist)
9. Serverrakendus väljastab tõendi andmed.
10. Digikukru rakendus signeerib oma privaatvõtmega tõendi (sh. kõik andmeväljad, mis on tõendis) ja edastab signatuuri serverrakendusele, et tõestada tõendi kättesaamist.
11. Serverrakendus verifitseerib esitatud signatuuri, märgib andmebaasis dokumendi väljastatuks (sh. salvestab andmebaasi informatsiooni konkreetsesse telefoni väljastatud tõendi metainfo kohta), ja vastab kinnitusega, et on tõestuse kätte saanud.
12. Digikukru rakendus kuvab kasutajale info tõendi tarnimise kohta.
13. Kasutaja loeb info ja annab rakenduses kinnituse.
14. Digikukru rakendus teeb päringu serverrakendusele, et saada tõendi terviklikkust kinnitavad autentimisvõtmed.
15. Serverrakendus tagastab tõendi autentimisvõtmed.
16. Digikukru rakendus kuvab infot autentimisvõtmete tarnimise kohta.

Märkused

1. Keelatud on sammude 13-17 vahelejätmine ning koheselt uue dokumendi tarnimise alustamine (s.t. sammust 3 jätkamine). Sellisel juhul jäävad dokumentide esitamiseks tarvilikud autentimisvõtmed tarnimata.

2. Samal ajal ei tohi mDL seadmesse paigaldada mitme eri isiku ID-kaarte. Kui seda teha, võivad tagajärjed olla ettearvamatud kasutuslugude toimimise mõttes.
3. Kui ebaõnnestub serverrakendusega ühenduse saamine sammus 3, tasub proovida, kas mobiiltelefoni brauserist (väljaspool digikukru rakendust) on võimalik saada ühendust serverrakendusega (aadressil http://<serveri_aadress>:<port>/admin).

Laiendid (Stsenaariumid, mis kirjeldavad lahknevusi peastsenaariumist ning võivad olla õnnestumised või nurjumised.)

-

Garantii

mDL formaadis tõend on väljaandja poolt signeeritud ja digikukru rakendusse tarnitud.

Lisainfo

Näidisrakenduses on kasutusmalli sammus 3 täidetavad tõendite tarnekoodid järgnevad:

- 1001 - ID-kaart, Mari-Liis Männik
- 2001 - ID-kaart, Jaak-Kristjan Jõeorg
- 2007 - Harrastuspüügiõigus, Jaak-Kristjan Jõeorg

2.4. Kasutusmall 04 - Vaata tõendi väljastamise ja uuendamisega seotud infot digikukru rakenduses

Tegijad

- Tõendi omanik
- Digikukru rakendus

Eeltingimused

Tõendi omaniku seadmes on installeeritud ja avatud digikukru rakendus, mis sisaldab vähemalt ühte tõendit.

Õnnestumise peastsenaarium

1. Tõendi omanik valib tõendi mille kohta soovib väljastamise ja uuendamisega seotud infot näha.
2. Digikukru rakendus kuvab järgneva info tõendi kohta:
    - Nimi
    - Tõendi tüüp
    - Tõendi digikukrusse lisamise kuupäev (päev, kuu,aasta, kellaaeg(tunnid,minutid,sekundid)).
    - Viimane uuenduste kontrollimise aeg
    - Viimane autentimisvõtmete uuendamise aeg

Laiendid (Stsenaariumid, mis kirjeldavad lahknevusi peastsenaariumist ning võivad olla õnnestumised või nurjumised.)

-

Garantii

Tõendi omanik on vaadanud tõendi väljastamisega seotud infot.

2.5. Kasutusmall 05 - Kustuta tõend digikukru rakendusest

Tegijad

- Tõendi omanik
- Digikukru rakendus
- Serverrakendus

Eeltingimused

Tõendi omaniku seadmes on installeeritud ja avatud digikukru rakendus, mis sisaldab vähemalt ühte tõendit ja ühendus serverrakendusega on loodud.

Õnnestumise peastsenaarium

1. Tõendi omanik valib tõendi, mida soovib kustutada.
2. Digikukru rakendus kuvab tõendi kustutamise valiku.
3. Tõendi omanik valib tõendi kustutamise valiku.
4. Digikukru rakendus saadab kustutamise päringu serverrakendusele.
5. Serverrakendus kustutab väljastatud tõendi märke.
6. Digikukru rakendus kustutab rakenduses asuva tõendi ja kuvab kustutamise info.

Laiendid (Stsenaariumid, mis kirjeldavad lahknevusi peastsenaariumist ning võivad olla õnnestumised või nurjumised.)

-

Garantii

Valitud tõend on kustutatud digikukru rakendusest.

3. Tõenditel olevad andmed

Näidistõenditena on kirjeldatud harrastuskalapüügiõigust tõendav tõend ja ID-kaart. mDL formaadil põhinevad digikukru ja kontrollija näidisrakendused peavad olema võimelised eristama, millise tõendiga on parasjagu tegemist. Selle võimaldamiseks on mDL spetsifikatsioonis parameeter `DocType`, mis ID-kaardi kontekstis peab omama väärtust `ee.eesti.1.3.6.1.4.1.51361.1.1.1.ID`. Ka harrastuskalapüügiõigust tõendava tõendi jaoks on vaja defineerida `DocType`; prototüüprakenduses oleme valinud selleks `ee.eesti.110072020095.1.hp` (siin "hp" viitab harrastuspüügile, "110072020095" viitab kalapüügiseaduse aktile ja "1" sellele, et tegemist on esimese versiooniga vastavast elektroonsest dokumendist).

Selleks, et mDL formaadil põhinev digikukru rakendus ja kontrollrakendus pakuksid tuge erinevatele dokumendiformaatidele, peavad mõlemad rakendused teadma, millistest nimeruumidest otsida vastava formaadi korral infot. ID-kaardi korral on kasutusel kaks nimeruumi:

- org.iso.18013.5.1 (standardne mDL nimeruum)
- org.iso.18013.5.1.EE (Eesti-spetsiifiline laiendus mDL nimeruum, sisaldab isikukoodi)

Harrastuskalapüügiõiguse korral kasutatakse järgmisi nimeruume:

- org.iso.18013.5.1 (sisaldab neid andmevälju, mis on ühised nii harrastuskalapüügiõigusele kui ka mDL formaadis juhiloale)
- org.iso.18013.5.1.EE (Eesti-spetsiifiline laiendus, sisaldab isikukoodi)
- ee.eesti.110072020095.1.hp (nimeruum, mis sisaldab kõiki harrastuskalapüügiõigusele spetsiifilisi andmevälju)

Mõlemad dokumendi puhul on isikukoodi jaoks kasutatud sama andmevälja (org.iso.18013.5.1.EE), et võimaldada dokumentide seostamist läbi isikukoodi andmevälja. Päris lahenduses võiks seostamine toimuda ETSI identifikaatori järgi, mitte isikukoodi järgi. Hetkel kasutati isikukoodi näidisrakenduses lihtsuse mõttes.

Dokumendi lisades on kirjeldatud, millised andmeväljad on näidistõendite puhul kasutusel. Lisa A kirjeldab ID-kaardi andmevälju, Lisa B harrastuskalapüügiõiguse tõendi andmevälju. Andmeväljade kirjeldusele järgnevad andmetabeli veergude selgitused (Lisa C). Nii ID-kaardile kui ka harrastuskalapüügiõiguse tõendile on lisatud andmeväljad *Väljaandja asutus* ja *Väljaandja riik*, mis nende tõendite peal hetkel ei ole. Nimetatud andmeväljad on lisatud, sest tulevikus võivad need olla olulised, et oleks tagatud koostalitlusvõime erinevate mDL formaadil põhinevate kontrollrakenduste ja digikukru rakenduste vahel. Lisaks on ID-kaardile lisatud andmeväljad *Vanus 18+* ja *Vanus 21+*, et demonstreerida, kuidas saab kontrollida tõendi omaniku vanuse olemist üle sätestatud piiri, avaldamata kontrollijale tõendi omaniku täpset vanust.

4. Teadaolevad rakenduse piirangud

Kuna käesoleva projekti näidisrakendused on omakorda ehitatud Google poolt loodud näidisrakenduste baasil, siis võivad teatud olukordades esineda tõrked. Google ei paku enda loodud näidisrakendustele garantiid, kuna tegemist ei ole Google ametliku tootega. Cybernetica on testinud põhivoogusid ja kaardistanud testimise käigus ilmnenud tõrkeolukorrad alljärgnevalt.

4.1. Tõrkeolukorrad, kui Bluetooth on välja lülitatud

Andmete vahetamine mobiilirakenduste vahel töötab Bluetooth režiimis. Kui Bluetooth on välja lülitatud või Bluetoothiga esineb probleem, võivad rakendused käituda ettearvamatult. Näiteks:

- Kui Bluetooth on välja lülitatud ning vajutada AppHolder rakenduses nuppu "Present documents", jookseb rakendus kokku.

4.2. Tõrkeolukorrad seotud BLE režiimi valikuga

- Kui QR kood on skanneeritud tuleb kontrollija rakenduses valida kahe BLE režiimi vahel. Kõigi seadmete puhul ei pruugi mõlemad režiimid toimida. Kui valitakse seadmele mittesobiv režiim siis ei looda ühendust. Tuleb vajutada 'Cancel' ja proovida ühenduse loomist eelnevast valikust erineva BLE režiimi vahel. Valikus on BLE:

central client mode: BLE seade, mis saadab ühenduse päringu teisele, ennast nähtavaks tegevale, *peripheral* seadmele.

peripheral server mode: BLE seade, mis teeb ennast nähtavaks ja võtab vastu ühenduse loomise päringu *central* seadme käest.

- Kui QR kood on skanneeritud aga kontrollija rakenduses ei pakuta BLE režiimi valikut siis on võimalik, et digikukru rakenduses on seadete alt vaja sisse lülitada mõlemad BLE režiimid. Selleks avada digikukru rakenduses seaded ja võimaldada mõlemad BLE režiimid.

4.3. Tõrgete lahendamine

Kui dokumendi tarnimisel mobiilirakendusse tuleb veateade `Cleartext HTTP traffic to … not permitted`, siis on jäänud tegemata järgnev samm rakenduse AppHolder paigaldusjuhendis:

- Mobiilirakendus suhtleb prototüübis serverrakendusega üle HTTP protokolli. Selleks, et seda Androidis võimaldada, on vaja lisada serverrakenduse domeeni kohta vastav rida faili:
- "appholder/src/main/res/xml/network_security_config.xml"

Viited

- [1] https://github.com/google/mdl-ref-apps
- [2] ISO/IEC DIS 18013-5. Personal identification — ISO-compliant driving licence — Part 5: Mobile driving licence (mDL) application

Lisa A: ID-kaardil kasutatavad näidisandmete komplektid

ID-kaardil esitatud andmeväljad (defineeritud `org.iso.18013.5.1` nimeruumis).

Identifikaator	Nimetus	Definitsioon	Kodeering
family_name	Perekonnanimi	ID-kaardi omaniku perekonnanimi.	tstr
given_name	Eesnimi	ID-kaardi omaniku eesnimi/-ed, teised nimed.	tstr
sex	Sugu	ID-kaardi omaniku sugu. Väärtus standardist ISO/IEC 5218.	tstr
birth_date	Sünniaeg	Päev, kuu, aasta, millal ID-kaardi omanik on sündinud.	full-date
issue_date	Välja antud	Päev, kuu, aasta millal dokument on välja antud.	full-date
expiry_date	Kehtiv kuni	Päev, kuu, aasta millal dokument kaotab kehtivuse.	full-date
nationality	Kodakondsus	ID-kaardi omaniku kodakondsust näitav kahekohaline tähtedest koosnev riigi kood. Defineeritud ISO-3166-1 standardis.	tstr
birth_place	Sünnikoht	ID-kaardi omaniku sünniriik (täispikk riigi nimetus).	tstr
document_number	Dokumendi number	Dokumendi number.	tstr
portrait	ID-kaardi omaniku foto	ID-kaardi omaniku portreefoto.	bstr
issuing_country	Väljaandja riik	Tõendi väljaandja asutuse asukohariigi kahekohaline riigi tähis vastavalt ISO 3166-1 standardile.	tstr
issuing_authority	Väljaandja asutus	Väljaandva asutuse nimetus.	tstr
age_over_18	Vanus 18+	Tõeväärtus, mis näitab, kas ID-kaardi omaniku vanus on 18 või rohkem eluaastat.	bool

Identifikaator	Nimetus	Definitsioon	Kodeering
age_over_21	Vanus 21+	Tõeväärtus, mis näitab, kas ID-kaardi omaniku vanus on 21 või rohkem eluaastat.	bool

ID-kaardile lisatavad andmeväljad (Eesti-spetsiifilises `org.iso.18013.5.1.EE` alamnimeruumis).

Identifikaator	Nimetus	Definitsioon	Kodeering
id_code	Isikukood	ID-kaardi omaniku isikukood.	tstr

Lisa B: Harrastuskalapüügiõiguse tõendil kasutatavad näidisandmete komplektid

Harrastuskalapüügiõiguse tõendil olevad andmeväljad, mis kuuluvad `org.iso.18013.5.1` nimeruumi.

Identifikaator	Nimetus	Definitsioon	Kodeering
family_name	Perekonnanimi	Tõendi omaniku perekonnanimi.	tstr
given_name	Eesnimi	Tõendi omaniku eesnimi/-ed, teised nimed.	tstr
issue_date	Välja antud	Päev, kuu, aasta, millal tõend on väljastatud.	full-date
expiry_date	Kehtiv kuni	Päev, kuu, aasta, millal tõend kaotab kehtivuse.	full-date
issuing_country	Väljaandja riik	Tõendi väljaandja asutuse asukohariigi kahekohaline riigi tähis vastavalt ISO 3166-1 standardile.	tstr
issuing_authority	Väljaandja asutus	Väljaandva asutuse nimetus.	tstr

Harrastuskalapüügiõiguse tõendile lisatavad andmeväljad (Eesti-spetsiifilises `org.iso.18013.5.1.EE` alamnimeruumis).

Identifikaator	Nimetus	Definitsioon	Kodeering
id_code	Isikukood	Püügiõiguse omaniku isikukood.	tstr

Harrastuskalapüügiõiguse tõendil olevad andmeväljad, mille me defineerime `ee.eesti.110072020095.1.hp` nimeruumis.

Identifikaator	Nimetus	Definitsioon	Kodeering
reg_nr	Registreerimisnumber	Tõendi registreerimisnumber.	tstr
phone_nr	Telefoni number	Püügiõiguse omaniku telefoninumber.	tstr
e-mail	e-post	Püügiõiguse omaniku e-posti aadress.	tstr
payment_date	Tasumise kuupäev	Päev, kuu, aasta, millal tõendi eest tasuti.	full-date

Identifikaator	Nimetus	Definitsioon	Kodeering
payment_amount	Tasumise summa	Püügiõiguse eest tasutud summa.	tstr

Lisa C: Andmetabelite veergude selgitused

Andmetabeli veergude selgitused (IS0-18013-5) [2]

- Identifikaatori veeru väärtust kasutatakse *DataElementIdentifier* väärtusena vallasrežiimise tõendi esituse puhul.
- Nimetus - eestikeelne nimetus identifikaatorile.
- Definitsioon - andmevälja selgitus.
- Kodeerimise veerg näitab, kuidas andmeelemente kodeerida. “tstr”, “uint”, “bstr”, “bool” ja “tdate” on CDDL esitustüübid nagu on RFC 8610-s. 'full-date' on defineeritud kui *full-date = #6.1004(tstr)*, kus 1004 on spetsifitseeritud RFC 8943.
  - RFC 7049 peatüki 2.4.1 kohaselt, *tdate* andmeobjekt peab sisaldama date-time stringi nagu spetsifitseeritud RFC 3339-s. RFC 8943 kohaselt *full-date* andmeobjekt peab sisaldama full-date stringi nagu on spetsifitseeritud RFC 3339-s
  - Järgnevad nõuded kehtivad kõikidele kuupäevade esitlustele mDL kuupäeva elementides kui pole teistmoodi viitatud:
    - Sekundite murdosasid ei kasutata;
    - kohaliku erinevust UTC suhtes ei tohi kasutada nagu on viitatud RFC 3339-s, seades *time-offset* väärtuseks "Z".