

Riigi autentimisteenuse (TARA) demokeskkonna liitumistaotlus

1. Soovime liituda Riigi autentimisteenuse (TARA) demokeskkonnaga.
2. Kinnitame, et kasutame demokeskkonda ainult testimise eesmärgil.
3. Kinnitame, et oleme tutvunud Riigi autentimisteenuse tehnilise [dokumentatsiooniga](#) ja arvestame RIA poolt kehtestatud [ärikirjelduses](#) toodud nõuete ning soovitustega oma klientrakenduse liidestamisel.
4. Palume:
 - registreerida meid TARA demokeskkonna kliendiks;
 - väljastada meile klientrakenduse identifikaator ja salasõna;
 - avada juurdepääs Riigi autentimisteenuse (TARA) demokeskkonnale.

Kliendi asutuse nimi või nimetus: Registrikood: Aadress: Telefon: E-post:	
Kontaktisiku nimi: Kontaktisiku e-post: Kontaktisiku telefon: Kontaktisiku isikukood: (klientrakenduse salasõna krüpteeritult saatmiseks)	
Tehniliste teavituste e-posti aadress(id):	
Katkestustest teavitamise e-posti aadress(id):	
Riigi autentimisteenuse kasutamise eesmärk: <i>nt avaliku ülesande kirjeldus, mille raames teenust edaspidi kasutada soovitakse või info kellele teenust arendatakse</i>	
Klientrakenduse nimetus: Kuvatakse kasutajale Riigi autentimisteenuse (TARA) autentimisvalikute lehel. Kasutada sama nimetust, mida klientrakenduse päises/pealkirjas kasutajale kuvatakse. <ul style="list-style-type: none">• Maksimaalne pikkus 150 tähemärki.• Lisada inglisi- ja venekeelsed tõlked juhul, kui nimetus on klientrakenduses tõlgitud. Loe nõuete kohta lähemalt siit .	
Klientrakenduse lühinimetus: Kuvatakse kasutajale mobiilseadmega autentimisel. Lühinimetus peab seostuma eelmisel väljal esitatud klientrakenduse nimetusega. <ul style="list-style-type: none">• Maksimaalne pikkus 20 - 40 tähemärki sõltuvalt kasutatud tähemärkidest.• Lisada inglisi- ja venekeelsed tõlked juhul, kui nimetus on klientrakenduses tõlgitud. Loe nõuete kohta lähemalt siit .	
Autentimismeetod(id), mida soovime kasutada:	

Autentimise tagasisuunamispäringus lubatud URL-id:

Väärtuseks peab olema [TARA tehnilisele spetsifikatsioonile](#) vastav klientrakenduse otpunkt (*OpenID Connect mõistes redirect uri*).

Pärast edukat autentimist või autentimise katkestamisel või autentimise vea korral suunatakse kasutaja veebisirvik sellele aadressile, pannes kaasa spetsifikatsioonis kirjeldatud URL parameetrid.

Märkus:

Iga väärtus peab vastama URL standardile, ei tohi sisaldada [kasutajainfo](#) (domeeninimele @ sümboliga eelnev osa) ega [fragmendi](#) osa (URL-is # sümbol ja sellele järgnev osa). Protokoll tohib olla ainult https.

Tõendipäringu autentimismeetod:

Tõendiväljastuse otpunkti (*OpenID Connect token päringu*) puhul klientrakenduses kasutatav *client authentication method*.

Vaikeväärtus on `client_secret_basic`. Kui on soov kasutada `client_secret_post`, siis märkida see.

Kliendi esindaja nimi ja amet

/digitaalselt allkirjastatud/