OpenID.ee teenuse tutvustus

Mart Randala
Mart Sõmermaa
Martin Paljak

OÜ Ideelabor

OpenID teenuse tutvustus

OpenID on autentimisprotokoll, mis võimaldab kasutada üht kasutajatunnust kõigil OpenID toega veebisaitidel. Lisaks autentimisele võimaldab OpenID protokoll edastada ka kasutaja isikuandmed (nimi, vanus, e-mail, sugu jne). OpenID.ee seob OpenID protokolli Eesti ID-kaardiga ja mobiil-IDga, tehes OpenID kasutamise lihtsaks ja turvaliseks.

OpenID raamistikku kasutavad teiste hulgas ka paljud suurfirmad: Google, Microsoft, Sun jpt. Selline avatud raamistik võimaldab teenusepakkujatel taaskasutada olemasolevaid kontosid erinevate veebiteenuste puhul (nn. *Federated Identity* kontseptsioon) ning pakkuda personaliseeritud kasutajakogemust ilma kasutajat uuesti autentimata (nn. *Single Sign-On*).

OpenID.ee on tavapärase OpenID teenuse edasiarendus – kasutaja andmete allikaks on riiklik ID-kaardi infrastruktuur. See lahendab mõned tavalised OpenID teenusepakkujate probleemid. ID-kaardi infrastruktuuri kasutamise tõttu saab OpenID.ee tagada, et:

- iga OpenID taga on reaalne isik,
- põhiandmed (nimi, sugu, vanus) on verifitseeritud,
- autentimine on turvaline, *man-in-the-middle* ja autentimistunnuste vargus pole võimalik.

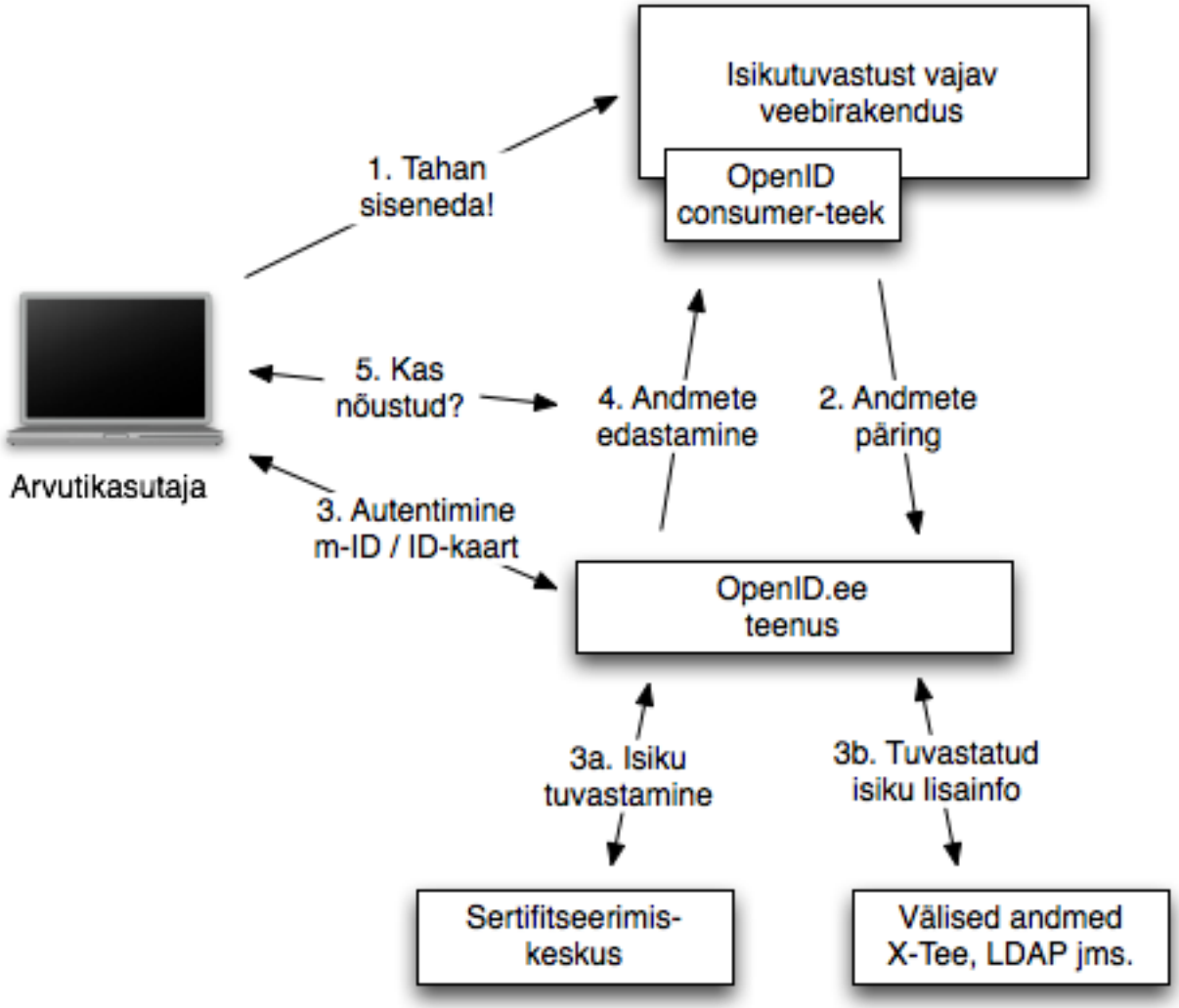
Vajadusel võimaldab teenus kasutaja andmeid pärida riiklikest registritest X-tee andmevahetuskihi abil.

OpenID.ee teenus on rakendatav olukordades, kus integreeritus riikliku infrastruktuuriga on vajalik (ID-kaart, Mobiil-ID; X-tee), kuid tehnilised võimalused selle teostamiseks on piiratud või ei ole otstarbekad. Integreerijale on mugav, sest OpenID.ee kasutamiseks on vajalik vaid OpenID teegi seadistamine veebirakenduses. Kasutajatele on mugav kasutada, sest konto registreerimist pole vaja.

Kasutajal on täielik kontroll edastatavate isikuandmete üle. OpenID.ee teenus edastab isikutuvastamisel kasutaja unikaalse tunnuse ja kasutaja poolt lubatud isikuandmed. Tunnuseid on kolme tüüpi:

- anonüümne
- pseudonüümne
- nimeline

OpenID teenuse ülevaade linnulennult



OpenID.ee kasutusvõimalused

1. **Anonüümne OpenID koos vabatahtlikult edastavate andmetega.**
    1. Klientrakendusele edastatakse kasutaja unikaalne identifikaator ning see ei eelda isikustatud andmete edastamist. Iga kasutaja saab võimaluse soovi korral enda isikut soovitud tasemeni avalikustada, kuid see pole kohustuslik.
    2. Sobiv rakendustes, kus on vajalik isiku unikaalsuse garanteerimine, kuid mitte isikustatud kasutajate nimekiri. Näiteks anonüümsed veebihääletused, kus on tähtis, et igal kasutajal oleks täpselt üks hääl ühe teema kohta.
2. **Anonüümne OpenID koos kohustuslikult edastavate andmetega.**
    1. Klientrakendusele edastatakse kasutaja unikaalne identifikaator koos kohustuslike väljadega, kuid see ei võimalda isikut tuvastada. Näiteks klientrakendus saab ainult väljad "sugu", "vanus" või "sünnikuupäev".
    2. Sobiv rakendustes, kus on vaja koguda andmeid kasutajate kohta statistilistel eesmärkidel ning isikutuvastus ei ole oluline. Näiteks online-küsitlused (suguline-vanuseline statistika vastajate kohta), doteeritud internet TÜ tudengitele vms.
3. **Pseudonüümne OpenID, mis on osaliselt isikustatud**
    1. Kasutaja valib unikaalse pseudonüümi
    2. Klientrakendusele edastatakse kasutaja unikaalne pseudonüüm koos pseudonüümsete andmetega. Kaasata võib online-profiile (MSN, Skype, Facebook, FOAF jms)
    3. Sobiv rakendustes, kus on vajalik isikute unikaalsus ning "seadistatav" profiil. Näiteks õpikeskkonnad ja/või sotsiaalsed võrgustikud, kus kasutajatel on oluline omada võimalust enda profiili kujundada-seadistada.
    4. ID-kaardi ja Mobiil-ID infrastruktuuri kasutamine tõstab turvalisust. Kui tegu on saitide võrgustikuga, siis OpenID.ee võimaldab kasutada kõiki saite ühe "kontoga".
4. **Isikustatud OpenID koos X-Tee andmetega**
    1. Autentimise transaktsiooni ajal päritakse X-Teest andmeid inimese kohta. Näiteks rahvastikuregister ja elukoht või Haridusministeerium ja EHIS. See võimaldab vastata küsimustele - kas inimene X on õpetaja? kas inimene Y on õpilane? Mis kooli(de)ga on inimene Z seotud?
    2. Sobiv rakendustes, kus on vajalik integreeritus riiklike registritega, kus on vaja operatiivselt sisulist infot kasutaja kohta; kuid võimalused ise ID-kaardi/Mobiil-ID infrastruktuuriga (ja X-Teega) liitumiseks on piiratud.
5. **Isikustatud OpenID - kõik ID-kaardi andmed edastatakse**
    1. Kõik isikuandmed edastatakse kasutaja nõusolekul. Sisuliselt on tegu tavalise ID-kaardi/Mobiil-ID autentimise analoogiga, mille turvalisus on võrdeline tava-ID-kaardi autentimisega. Lisaväärtus - toeatud on maksimaalne tehniliste tarbijate skoop nii ID-kaardi kui ka Mobiil-ID tarbijate seas.
    2. Lõpptarbijale jääb andmete edastamise kohta valik "nõustun" ja "ei nõustu".
    3. Veebirakendusel pole vaja SSL sertifikaati ID-kaardi ega lepingut mID veebiteenuse kasutamiseks.