Identiteetitagamisprofiil

Dokument	TAAT Identiteeditagamisprofiil
Identifikaator (OID)	1.3.6.1.4.1.19974.12.2.1.3
Versioon	1.3
Viimati muudetud	05.09.2012

1. Identiteedipakkujale kehtivad nõuded
    1.1 Lõppkasutaja autentimine
    1.2 Kasutajate registreerimine ja isikutuvastus
    1.3 Nõuded kasutajanimedele
    1.4 Nõuded paroolidele
    1.5 Andmete ajakohasus
    1.6 Kasutajakontode haldamine
    1.7 Rollid
2. Teenusepakkujale kehtivad nõuded
    2.1 TAATi kaudu vastu võetud andmete säilitamine ja kasutamine
3. Kõigile Föderatsioonis Osalejatele kehtivad nõuded
    3.1 Turvalisus

1. Identiteedipakkujale kehtivad nõuded

Nõudeid, mis esitatakse ainult TAATile edastatavatele kasutajakontodele. Nõuete täitmine konkreetses asutuses peab olema kirjeldatud Identiteedihalduse Aruandes.

1.1 Lõppkasutaja autentimine

1.1.1 Kasutajakonto peab viitama täpselt ühele füüsilisele isikule (Lõppkasutaja).

1.1.2 Lõppkasutajat võib infosüsteemides autentida kasutades ID-kaarti, Mobiil-ID või kasutajanime ja parooli, mille puhul kehtivad tingimused punktides 1.3-1.4.

1.2 Kasutajate registreerimine ja isikutuvastus

1.2.1 Kasutajakontoga seotud isikuandmed peavad pärinema usaldusväärsest allikast: isiku enda antud andmed või Identiteedipakkuja poolt usaldatud registrist (sh SAIS), mis juhul vastutus andmete õigsuse eest jääb Identiteedipakkujale.

1.2.2 Isiku tuvastamiseks tuleb kasutada ühte järgnevatest:

- näost näkku kohtumine ning isikut tõendava dokumendi esitamine
- ID-kaardiga autentimine
- Mobiil-ID
- Panga kaudu autentimine

1.2.3 Kasutajatunnused ja paroolid tohib üle anda vaid tuvastatud kontoomanikule

1.3 Nõuded kasutajanimedele

1.3.1 Kasutajanimi peab olema unikaalne igal ajahetkel.

1.3.2 Kasutajanimede korduvkasutamine on lubatud kui eelnev unikaalsuse nõue on tagatud.

1.4 Nõuded paroolidele

1.4.1 Parool peab olema vähemalt 6 (soovituslikult 8 või rohkem) sümbolit pikk ning kasutama vähemalt ühte järgmistest meetmetest:

- Sisaldab nii suuri kui väikseid tähti
- Sisaldab nii tähti kui numbreid

- Sisaldab erisümboleid (kirjavahemärke)

1.4.2 Kasutusel peavad olema baasmeetmed äraarvamise vastu (nt ei ole lubatud kasutada paroolina oma kasutajatunnust või eesnime).

1.4.3 Parooli ei ole lubatud säilitada või logida avatekstina.

1.5 Andmete ajakohasus

1.5.1 Identiteedipakkuja on vastutav kasutajaga seotud andmete ajakohasuse eest.

1.6 Kasutajakontode haldamine

1.6.1 Iga Lõppkasutaja konto peab omama läbi ajaloo unikaalset identifikaatorit.

1.6.2 Identifikaatori muutumisel peab olema tuvastatav side varasemaga.

1.6.3 Kasutajaandmed võivad olla kättesaadavad ainult töötajale, kelle tööülesannete hulka kuulub kasutajakontode käitlemine.

1.6.4 Kasutaja peab olema teavitatud tema parooli konfidentsiaalsuse nõudest.

1.6.5 Kui tuvastatakse parooli leke, on Identiteetipakkujal kohustus parool esimesel võimalusel vahetada või konto lukustada.

1.6.6 Parooli või kasutajatunnuse ununemise puhul tuleb ligipääsu taastamiseks isik tuvastada vastavalt punktis 1.2.2 esitatud nõuetele. Avatekstina võib kasutajale saata vaid ühekordseid paroole või paroolivahetamisvõtmeid.

1.7 Rollid

1.7.1 Iga aktiivne kasutajakonto peab olema seotud vähemalt ühe rolliga, mis vastab tema positsioonile asutuses.

1.7.2 Kui isiku rollid asutuses muutuvad või lõppevad (eksmatrikuleerimine, töölepingu lõpp, tööülesannete muutumine jm), peab tema kontoga seotud rolle uuendama 14 päeva jooksul.

2. Teenusepakkujale kehtivad nõuded

2.1 TAATi kaudu vastu võetud andmete säilitamine ja kasutamine

2.1.1 Teenusepakkujal on TAATi kaudu vastu võetud andmeid õigus säilitada ja kasutada vaid EENetiga sõlmitud lepingus loetletud teenuste osutamiseks.

2.1.2 Kui Teenusepakkuja kasutab ka kohalikku autentimissüsteemi, mille kaudu on võimalik ligipääs TAATi kaudu vastu võetud andmetele, laienevad sellele autentimissüsteemile tingimused puntkides 1.1, 1.3 ja 1.4.

3. Kõigile Föderatsioonis Osalejatele kehtivad nõuded

3.1 Turvalisus

3.3.1 Kõik Lõppkasutajaga seotud andmed peavad olema krüpteeritud, kui neid edastatakse üle avatud võrgu, kusjuures kasutatavate võtmete minimaalne tugevus peab olema 2048 bit RSA või sellega võrreldav standard.

3.3.2 Autentimismehhanisme peab kaitsma levinud rünnakute vastu nagu pealtkuulamine, vahemehe-rünne (*man in the middle attack*) või parooli arvamine.

3.3.3 Kasutatav tark- ja riistvara peab vastama kaasaegsetele turvanõuetele, sealhulgas tootjapoolseid turvauuendusi peab rakendama esimesel võimalusel.

3.3.4 Füüsiline ligipääs kasutajaandmeid ja nende varundusi sisaldavatele riistvarale peab olema lubatud ainult töötajale, kelle tööülesannete hulka kuulub riistvara või kasutajaandmete haldamine. Kõrvaliste isikute ligipääs on lubatud ainult eelnimetatud töötajate vastutusel.

3.3.5 Maha kantud riist- ja tarkvarast, mis sisaldavad kasutajaandmeid, tuleb vabaneda viisil, mis välistavad sealt andmete taastamise.

3.3.6 Kõik kasutajaandmetele kehtivad nõuded laienevad neid andmeid sisaldavatele logidele.