



## 1. LIITE 1 – ENNEN LIITTYMISTÄ TOIMITETTAVAT TIEDOT

### 1.1. Selvitys Kotiorganisaatioksi liittymisestä

Ennen kuin Jäsen voi aloittaa Kotiorganisaationa toimimisen, sen on toimitettava Opetushallitukselle seuraavat tiedot:

#### Yhteystiedot

- Hallinnollisen yhteyshenkilön nimi, puhelinnumero ja sähköpostiosoite
- Teknisen yhteyshenkilön nimi, puhelinnumero ja sähköpostiosoite
- Tietosuojavastaavan nimi, puhelinnumero ja sähköpostiosoite

### 1.2. Selvitys Palveluntarjoajaksi liittymisestä

Ennen kuin Jäsen voi aloittaa Palveluntarjoajana toimimisen, sen on toimitettava Opetushallitukselle seuraavat tiedot:

#### Yhteystiedot

- Hallinnollisen yhteyshenkilön nimi, puhelinnumero ja sähköpostiosoite
- Teknisen yhteyshenkilön nimi, puhelinnumero ja sähköpostiosoite
- Tietosuojavastaavan nimi, puhelinnumero ja sähköpostiosoite

#### Tunnistuksenvälityspalveluun liitettävät palvelut

- Loppukäyttäjille Luottamusverkoston välityksellä tarjottaviksi tulevat palvelut
- Palvelukohtaisesti eriteltyinä
  - Kuvaus palvelusta ja siitä, miten se tukee opetuksen tai koulutuksen järjestämistä
  - Linkki palveluntarjoajan sivulle
  - Kuvaus palvelun sisältämästä henkilötietojen käsittelystä
  - Palvelun asianmukaisen käytön edellyttämät toimenpiteet, mikäli tarpeen
  - Linkki Loppukäyttäjiä sitoviin käyttöehtoihin
- Linkki julkisesti saatavilla olevaan rekisteriselosteeseen, tietosuojaselosteeseen tai muuhun dokumenttiin, jossa henkilötietojen käsittely selostetaan



## 2. LIITE 2 – JÄSEN- JA TIETOTURVAVAATIMUKSET

Tässä liitteessä kerrotaan Luottamusverkoston jäsenen tietoturva-vaatimukset.

### 2.1. Kaikille yhteiset tietoturva-vaatimukset

#### Vastuutahot

- Jäsenellä on tietoturva-asioista vastaava vastuuhenkilö, kuten tietoturvavastaava, jolla on sekä kyky että valtuudet lievittää, hillitä tai rajoittaa tietoturvaloukkausten vaikutuksia organisaatiossa.

#### Tietoturvaloukkausten ehkäisy ja ohjelmistojen ajanmukaisuus

- Jäsenellä on ohjelmistojen haavoittuvuuksien havaitsemista ja korjaamista varten tehokas prosessi, jota se myös noudattaa.
- Jäsen pitää ylläpitämiensä käyttöjärjestelmien ja sovellusohjelmien tietoturvapäivitykset jatkuvasti ajantasaisina.

#### Kyky reagoida tietoturvaloukkauksiin

- Jäsenellä on mekanismi/mekanismit mahdollisten tietoturvaloukkausten havaitsemiseksi sekä tietojärjestelmien suojaamiseksi uhilta.
- Jäsenellä on tietoturvaloukkauksiin reagoimista varten toimintaohje, jota se myös noudattaa.
- Jäsen tallentaa järjestelmälokit, mukaan lukien tarkat aikaleimat ja järjestelmän komponenttien ja toimijoiden tunnukset, tietoturvaloukkausten selvittämisen mahdollistamiseksi. Lokitietoja käsitellään organisaation tietoturvaohjeiden ja -käytäntöjen mukaisesti.

### 2.2. Kotiorganisaatiota koskevat vaatimukset

#### Toimenpiteet ja toimenpidevalmiudet

- Kotiorganisaatio tiedottaa Loppukäyttäjille Tunnistuksenvälityspalvelusta ja sen kautta saavutettavissa olevien palveluiden käyttöä koskevista käyttöehdoista ja -säännöistä.
- Kotiorganisaatiolla on keino ottaa yhteys tiettyyn Loppukäyttäjään.
- Kotiorganisaatio pyrkii varmistamaan, että Loppukäyttäjät käyttävät palveluita lain ja hyvän tavan mukaisesti.
- Loppukäyttäjille luovutettavat käyttäjätunnukset tai muut tunnistusvälineet ovat riittävän suojattuja käyttötarkoitukseensa nähden.
- Kotiorganisaatiolla on mekanismi, jolla se voi rajoittaa tai muuttaa Loppukäyttäjän valtuuksia taikka poistaa ne kokonaan.
- Kotiorganisaatio pitää käyttäjähallintonsa jatkuvasti ajantasaisena, mukaan lukien vanhentuneiden, puutteellisten tai virheellisten tietojen poistaminen.
- Kotiorganisaatiolla on ajantasaisen käyttäjähallinnon lisäksi toimiva mekanismi, jolla estetään sen toiminnan piiristä poistuneiden Loppukäyttäjien henkilötietojen välittäminen Tunnistuksenvälityspalveluun ja/tai Palveluntarjoajille.
- Loppukäyttäjien kielletty toiminta (ks. alla) on sanktioitu.



## Käytösäännöt

Kotiorganisaatio on laatinut Loppukäyttäjille sen tarjoamaa tieto- ja viestintäteknikkaa sekä sähköisiä palveluita koskevat kirjalliset käytösäännöt, jotka täyttävät seuraavat vaatimukset:

- Tieto- ja viestintäteknikan käyttötarkoitus opetuksen tai koulutuksen järjestämisessä on määritelty.
- Loppukäyttäjältä edellytetään henkilökohtaisen käyttäjätunnuksen ja salasanan tai muiden tunnistusvälineiden huolellista käsittelyä.
- Luottamusverkoston kautta saatavilla olevien palveluiden tai sisältöjen käyttäminen muuhun kuin oppimis- tai opetustarkoitukseen on kielletty.
- Loppukäyttäjän on ilmoitettava havaitsemistaan väärinkäytöksistä opetuksen tai koulutuksen järjestäjän määrittelemälle taholle.
- Loppukäyttäjältä kielletään selkeästi kaikki sellainen Luottamusverkoston ja sen kautta saavutettavissa olevien palveluiden käyttö tai niiden kautta tapahtuva toiminta, joka rikkoo lakia, loukkaa kolmansien osapuolien oikeuksia tai hyvää tapaa taikka muutoin voi vaarantaa Luottamusverkoston tai sen kautta saavutettavien palveluiden toimintavarmuuden, tietoturvan tai tietosuojan. Tällaista kiellettyä käyttöä tai toimintaa ovat esimerkiksi
  - Laittomien aineistojen tallettaminen, jakaminen taikka tekijänoikeuden tai muiden immateriaalioikeuksien loukkaaminen
  - Herjaavien tai häiritsevien viestien, kuten roskapostin, lähettäminen tai julkaisu
  - Virusten tai muiden haittaohjelmien käyttö tai levittäminen
- Loppukäyttäjän on allekirjoituksellaan vakuutettava tutustuneensa käytösääntöihin.

### 2.3. Palveluntarjoajia koskevat vaatimukset

#### Palveluntarjoajaksi hyväksymisen edellytykset

- Palveluntarjoaja tarjoaa opetuksen tai koulutuksen järjestäjille sähköisiä työvälineitä opetuksen tai koulutuksen järjestämiseksi.
- Palveluntarjoaja toteuttaa asianmukaiset tekniset ja organisatoriset toimenpiteet Loppukäyttäjien henkilötietojen käsittelyn lainmukaisuuden, turvallisuuden ja luottamuksellisuuden varmistamiseksi.
- Palveluntarjoaja ei luovuta vastaanottamiaan henkilötietoja eteenpäin tai yhdistä niitä muihin hallussaan oleviin henkilötietoihin, mikäli Kotiorganisaation ja/tai Loppukäyttäjän ja Palveluntarjoajan välillä ei ole muuta sovittu.

#### Luottamusverkostoon liitettävien palveluiden vaatimukset

- Palvelu tukee opetuksen tai koulutuksen järjestämistä.
- Henkilötietojen käsittelyn oikeusperusteen lakattua Loppukäyttäjää koskevat henkilötiedot poistuvat tai poistetaan palvelusta viipymättä, mikäli Kotiorganisaation ja/tai Loppukäyttäjän ja Palveluntarjoajan välillä ei ole muuta sovittu.



### 3. LIITE 3 – TIETOMALLI

MPASSid-tunnistuksenvälityspalvelu välittää palveluille seuraavat käyttäjätiedot (teknisesti SAML-attribuutit) tunnistetuiista käyttäjistä. Yksityiskohtaisempi tekninen kuvaus on julkaistu osoitteessa <https://wiki.eduuni.fi/display/CSCMPASSID/MPASSid+Home> . Mikäli osoite muuttuu Opetushallitus ilmoittaa siitä jäsenille.

- Sukunimi (urn:oid:2.5.4.4)
- Etunimi (urn:oid:2.5.4.42)
- Yksilöllinen tunniste (urn:mpass.id:uid)
- CryptID (urn:mpass.id:legacyCryptId)
- Vahvennettu CryptID (urn:mpass.id:legacyCryptIde)
- Kuntakoodi (urn:mpass.id:municipalityCode) – poistuu käytöstä vuoden 2022 alusta lähtien.
- Kunnan nimi (urn:mpass.id:municipality) – poistuu käytöstä vuoden 2022 alusta lähtien.
- Koulukoodi (urn:mpass.id:schoolCode)
- Koulun nimi (urn:mpass.id:school)
- Luokka (urn:mpass.id:class)
- Vuosiluokka (urn:mpass.id:classLevel)
- Rooli (urn:mpass.id:role)
- Rooli 1.1 (urn:mpass.id:role\_v1.1) – poistuu käytöstä vuoden 2022 loppuun mennessä.
- Oppijanumero (urn:oid:1.3.6.1.4.1.16161.1.1.27)
- Opetuksen tai koulutuksen järjestäjän oid (urn:mpass.id:educationProviderId)
- Opetuksen tai koulutuksen järjestäjän nimi (urn:mpass.id:educationProvider)



## 4. LIITE 4 – OPETUSHALLITUKSEN PALVELUTASO

### 4.1. Yleinen palvelutaso

- Tunnistuksenvälityspalvelun yhteyspiste on [mpass@oph.fi](mailto:mpass@oph.fi). Mikäli yhteyspiste muuttuu Opetushallitus ilmoittaa siitä jäsenille.
- Opetushallituksen asiantuntijat ovat poikkeustilanteita lukuun ottamatta tavoitettavissa klo 8.30–16.00.
- Palvelupyynnöt käsitellään kiireellisyysjärjestyksessä.
- Opetushallitus kehittää ja testaa MPASSid-palvelua ja ohjelmakomponentteja, joiden avulla Jäsenet voivat kytkeytyä Tunnistuksenvälityspalveluun.
- Opetushallitus järjestää Jäsenten teknisille yhteyshenkilöille neuvontapalvelua toiminnallisten ongelmien selvittämiseksi.
- Opetushallitus ilmoittaa Jäsenille turvapäivityksistä tai -paikkauksista sekä pyrkii muutoinkin pitämään Luottamusverkoston turvallisena.
- Opetushallitus kokoaa MPASSid-tietomallia koskevat muutospyynnöt tai -tarpeet ja valmistelee niiden pohjalta muutokset.
- Opetushallitus antaa täsmentäviä ohjeita tietomallin käytöstä sekä eri attribuuttien syntaksista ja semantiikasta.
- Opetushallituksen ylläpitämä loki sisältää käyttäjän kotihakemiston yksilöllisen tunnisteeseen, jonka avulla käyttäjä voidaan yhdistää palveluntarjoajan tekniseen tunnisteeseen. Lisäksi tallentuu tieto Kotiorganisaation käyttäjähakemistosta.

### 4.2. Huoltotoimenpiteet ja huoltokatkot

- Ennakolta suunnitellut huoltokatkot ajoitetaan opetuksen tai koulutuksen järjestäjien normaalin virka-ajan ulkopuolelle.
- Opetushallitus ilmoittaa huoltotoimenpiteistä etukäteen lukuun ottamatta tilanteita, jotka edellyttävät yllättäviä ja välittömästi suoritettavia toimenpiteitä.
- Palvelun saatavuutta eivät rasita vähintään viikkoa etukäteen ilmoitetut katkot tai sovitut kuukausittaiset tai viikoittaiset palvelukatkot tai kriittisten tietoturvakorjausten suorittamisesta aiheutuvat katkot eivätkä kolmansista osapuolista johtuvat katkot.
- Opetushallituksen laitetilaympäristöön tai laitteistoon liittyvät huoltotoimenpiteet voivat aiheuttaa häiriöitä Tunnistuksenvälityspalveluun.
- Opetushallitus voi sulkea pääsyn Tunnistuksenvälityspalveluun välittömästi ja ilman ennakoilmoitusta havaittuaan tai saatuaan epäilyn palvelussa olevasta tietoturvapoikkeamasta riippumatta siitä, mikä taho tietoturvapoikkeaman on aiheuttanut.



## 5. LIITE 5 – HENKILÖTIETOJEN KÄSITTELY

### 5.1. Osapuolten roolit

- Kotiorganisaatio huolehtii henkilötietojen käsittelystä ja tietosuojaa koskevan lainsäädännön mukaisista rekisterinpitäjän vastuista ja velvollisuuksista.
- Opetushallitus toimii henkilötietojen käsitteijänä, joka käsittelee henkilötietoja rekisterinpitäjänä toimivan Kotiorganisaation lukuun.
- Opetushallitus toimii rekisterinpitäjänä Tunnistuksenvälityspalvelun lokitietojen ja Luottamusverkoston jäsenten yhteystietojen osalta.
  - Opetushallitus käsittelee rekisterinpitäjänä MPASSid:n lokitietoja ongelmatilanteiden ja tietoturvaloukkauksien selvittelyä varten.
  - Opetushallitus käsittelee rekisterinpitäjänä Luottamusverkoston jäsenten yhteystietoja Luottamusverkoston ja Tunnistuksenvälityspalvelun käyttöä koskevaa toimintaa varten.

### 5.2. Käsiteltävät henkilötiedot ja käsittelyn tarkoitus

- Opetushallitus käsittelee Kotiorganisaation lukuun ainoastaan MPASSid-tietomallin mukaisia henkilötietoja, jotka on kuvattu Liitteessä 3 tunnistuksenvälittämistä varten.
- Opetushallitus ei käsittele arkaluonteisia tai erityisiin henkilötietoryhmiin kuuluvia henkilötietoja.
- Opetushallituksen palvelimet sijaitsevat Suomessa, EU:n tai ETA-maassa.
- Opetushallitus ei käsittele tietomallin mukaisia tietoja muihin tarkoituksiin kuin Tunnistuksenvälityspalvelun tarjoamista varten eikä Opetushallitus tallenna tietoja, ota niistä varmuuskopioita tai tee niistä muitakaan tallenteita.

### 5.3. Opetushallituksen vastuut ja velvollisuudet

- Opetushallitus käsittelee henkilötietoja vain ja ainoastaan MPASSid-luottamusverkoston jäsensopimuksen, tämän liitteen tai Kotiorganisaation antamien muiden ohjeiden mukaisesti.
- Opetushallitus ei käytä Tunnistuksenvälityspalvelun Kotiorganisaation rekisteristä kysymiä henkilötietoja muussa toiminnassaan, yhdistele niitä muihin hallussaan oleviin tietoihin tai luovuta niitä muille kuin Palveluntarjoajille.
- Kotiorganisaatio voi Opetushallitukselle tehtävällä ilmoituksella rajoittaa niitä palveluita ja Palveluntarjoajia, joille sen Loppukäyttäjien henkilötietoja voidaan välittää.
- Opetushallituksen alaisuudessa olevat henkilöt ovat sitoutuneet noudattamaan salassapitovelvollisuutta sekä käsittelemään henkilötietoja ainoastaan MPASSid-luottamusverkoston jäsensopimuksen ja tämän liitteen mukaisesti.
- Opetushallitus huolehtii asianmukaisten teknisten ja organisatoristen toimien täytäntöönpanosta siten, että käsittely täyttää EU:n yleisen tietosuojasetuksen vaatimukset ja varmistaa rekisteröidyn oikeuksien suojelun.
- Opetushallitus toteuttaa asianmukaiset tekniset ja organisatoriset toimenpiteet käsittelyn riittävän turvallisuustason varmistamiseksi. Riittävän turvallisuustason arvioinnissa otetaan huomioon uusin tekniikka ja toteuttamiskustannukset, käsittelyn laajuus, asiayhteys ja tarkoitukset sekä



luonnollisten henkilöiden oikeuksiin ja vapauksiin kohdistuvat, todennäköisyydeltään ja vakavuudeltaan vaihtelevat riskit.

- Opetushallitus ei käytä toisen henkilötietojen käsittelijän palveluksia, ellei tästä ole kirjallisesti ja ennakolta sovittu Kotiorganisaation kanssa. Sopimuksen allekirjoitushetkellä Opetushallitus käyttää CSC – Tieteen tietotekniikan keskus Oy:tä henkilötietojen käsittelyssä. Kotiorganisaatio hyväksyy tämän alihankkijan käytön allekirjoittaessaan sopimuksen.
- Opetushallitus auttaa mahdollisuuksiensa mukaan Kotiorganisaatiota rekisteröidyn oikeuksien käyttämistä koskeviin pyyntöihin vastaamisessa. Opetushallitus voi tarvittaessa avustaa Kotiorganisaatiota esimerkiksi rekisteröidyille suunnatussa tiedotuksessa, viestinnässä tai pääsyoikeuden toteuttamisessa.
- Opetushallitus auttaa Kotiorganisaatiota varmistamaan, että käsittelyn turvallisuutta, tietoturvaloukkausten ilmoitusvelvollisuutta, vaikutustenarvioinnin laatimista ja ennakkokuulemista koskevat velvoitteita noudatetaan ottaen huomioon käsittelyn luonteen ja Opetushallituksen saatavilla olevat tiedot.
- Opetushallitus on valmis saattamaan Kotiorganisaation saataville tiedot, jotka ovat tarpeen sen lakisääteisten velvoitteiden noudattamisen osoittamiseksi, ja sallii Kotiorganisaation tai tämän valtuuttaman auditoijan suorittamat auditoinnit sekä osallistuu niihin.
- Opetushallitus ilmoittaa tietoonsa tulleista tietoturvaloukkauksista ilman aiheetonta viivytystä.
- Opetushallitus ylläpitää selostetta käsittelytoimista, joita se suorittaa Kotiorganisaation lukuun.