

# Sirtfi-itsearviointi (v2)

- [Sirtfi-itsearviointiprosessi](#)
- [Itsearviointin suorittaminen](#)
- [Sirtfi-tiedon päivittäminen resurssirekisterissä IdP:lle / SP:lle](#)



## HUOM!

Tämä on **Sirtfi v2** ohjeistus. Tämän version käyttö on **suositeltavaa**.

REFEDS Sirtfi (Security Incident Response Trust Framework for Federated Identity) -kehikolla on ennaltaehkäisevä sekä reaktiivinen vaikutus luottamusverkostossa tapahtuviin tietoturvapoikkeamiin. Ennaltaehkäisevästi toimijat tekevät kehikon mukaisen itsearviointin. Reagointi tietoturvapoikkeamiin edellyttää usein ripeää viestintää luottamusverkoston toimijoiden välillä, jonka edistämiseksi toimijat julkaisevat yhteystiedot luottamusverkoston metadatatassa.

Palveluorganisaatiot sitoutuvat Haka-luottamusverkostoon liittyessään voimassa olevaan [CoCo](#) käytännesääntöön, jossa edellytetään Sirtfi käyttöönottoa.

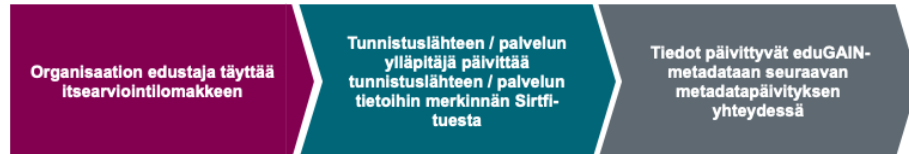
**Lisätietoa:** [SIRTFI – REFEDS](#)

## Sirtfi-itsearviointiprosessi

Organisaatio voi osoittaa toimivansa Sirtfi-kehikon vaatimusten mukaisesti suorittamalla itsearviointin. Itsearviointin suorittaminen on tarpeellista vain eduGAIN-luottamusverkostoon kuuluvilla organisaatioilla, mutta suositeltavaa kaikille Haka-luottamusverkostoon kuuluvilla organisaatioilla. Itsearviointi tehdään organisaatiokohtaisesti.

Organisaation edustaja (tietoturvan edustaja tai hallinnollinen yhteyshenkilö) täyttää Sirtfi-lomakkeen, jossa on 18 väittämää. Jos itsearviointin kaikkiin väittämiin valitaan vastaukseksi True, organisaatio täyttää Sirtfi-vaatimuksenmukaisuuden (18/18). Tällöin organisaation tunnistuslähteisiin tai palveluihin voidaan tehdä merkintä Haka-resurssirekisterissä Sirtfi-vaatimuksenmukaisuuden osoittamiseksi. Mikäli haluatte päivittää hallinnollisen yhteyshenkilön tai tietoturvan edustajan tietoja, olkaa yhteydessä [haka@csc.fi](mailto:haka@csc.fi).

Itsearviointia ei tarvitse suorittaa säännöllisesti, vaan Sirtfi-prosessi lähtee oletuksesta, että itsearviointi on ajantasainen. Organisaation vastuulla on huolehtia itsearviointin ajantasaisuudesta ja päivittää sitä tarvittaessa. Mikäli itsearviointin tulos päivityksen jälkeen ei täytä Sirtfi-vaatimuksenmukaisuutta (18/18), on organisaation vastuulla huolehtia, että organisaation tunnistuslähteet / palvelut päivitetään vastaamaan itsearviointin tulosta Haka-resurssirekisterissä.

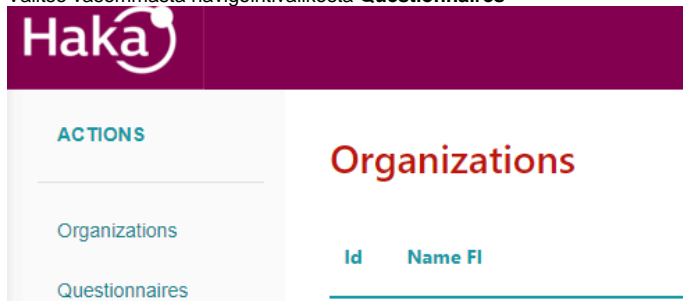


## Itsearviointin suorittaminen



Mikäli organisaatiosi on jo suorittanut itsearviointin, voit siirtyä kohtaan [Sirtfi-tiedon päivittäminen resurssirekisterissä IdP:lle / SP:lle](#)

- Kirjaudu osoitteeseen <https://rr.funet.fi/haf>
- Valitse vasemmasta navigointivalikosta **Questionnaires**



- Itsearviointilomake aukeaa (kuva alla). Lomakkeella on 18 väittämää itsearviointia suorittavan organisaation tietoturvakäytäntöihin liittyen. Kysymyksiin vastataan **True**, **False** tai **N/A**.

## Sirtfi v 2.0 Questionnaire (<https://refeds.org/sirtfi>)

### Operational Security [OS]

#### OS1 -

Security patches in operating system and application software are applied in a timely manner.

Comment (Consider this as a public information [for own use, only saved to database])

Answer

☐

False

☐ N/A

☐ True

#### OS2 -

A process is used to manage vulnerabilities in software operated by the organisation.

Comment (Consider this as a public information [for own use, only saved to database])

Answer

☐

False

☐ N/A

☐ True

- Lomakkeen lopussa kysytään yhteystietoja tietoturva-asioihin liittyen. Täytä osoitteeseen nimi ja sähköpostiosoite. Osoite pitäisi olla ns. prosessiosoite, esimerkiksi Security Team / [security@organisaatio.fi](mailto:security@organisaatio.fi)

### Security contact [CSC]

#### SIRTFICSC1 - Security contact name

Security contact name

Comment (Consider this as a public information [this information will be stored to metadata])

Answer

☐

False

☐ N/A

☐ True

#### SIRTFICSC2 - Security contact email

Security contact email

Comment (Consider this as a public information [this information will be stored to metadata])

Answer

☐

False

☐ N/A

☐ True

Submit

- Paina lopuksi Submit.
- Organisaation osalta Sirtfi-kysely on suoritettu ja voidaan siirtyä seuraavaan kohtaan.

## Sirtfi-tiedon päivittäminen resurssirekisterissä IdP:lle / SP:lle

Kun Sirtfi-kysely on täytetty, tunnistuslähteen tai palvelun ylläpitäjä voi Haka-resurssirekisterissä päivittää tiedon Sirtfi-kehikon mukaisten tietoturvakäytäntöjen noudattamisesta haluamissaan tunnistuslähteissä tai palveluissa.

- Kirjaudu Haka-resurssirekisteriin
- Avaa Manage IdPs tai Manage SPs ja avaa haluamasi IdP / SP
- Päivitä merkintä Sirtfi v2 -tuesta. Mikäli organisaatiosi ei ole vielä suorittanut itsearviointia, valinta on harmaana.

#### Sirtfi v2 (The Security Incident Response Trust Framework for Federated Identity) [18/18]

To enable Sirtfi v2 support (preferred), you have to fulfill all the Sirtfi requirements for this entity. Please visit [Sirtfi homepage](#) for more information.

Sirtfi v2 supported by this Identity Provider: **False**

☐

Apply Sirtfi v2

- Tallenna muutokset painamalla **Apply Sirtfi v2**
- Tallenna muutospyyntö painamalla **Submit IdP / SP Description**



Cancel modifications



Submit SP Description (unchanged)



Approve SP Description (unchanged)

- Haka-operaattori hyväksyy muutoksen ja se **julkaistaan eduGain-metadataan seuraavan metadatatäivityksen yhteydessä.**
- Tarkista vielä muokatun IdP:n eduGain-säännöt, mikäli haluat suodattaa eduGain-metadasta vain palvelut, jotka ovat Sirtfi-vaatimuksenmukaisia. (ks. [Ohje](#))

 Requested Attributes (unchanged)

 eduGain Rules (unchanged)