26.11.2019

Liite 5: Kansalaishavaintojärjestelmän toiminnan tekninen kuvaus

Johdanto

Tämä liite sopimukseen kansalaishavaintojen käyttöoikeudesta joukkoistamispalveluita varten on tarkoitettu selventämään ja täsmentämään kansalaishavaintojärjestelmän ja sitä hyödyntävien joukkoistamisjärjestelmien toimintaperiaatteita ja niiden välistä työnjakoa. Liite on tarkoitettu yleiseksi kuvaukseksi, joten mahdollisten ristiriitojen ilmetessä muiden sopimusasiakirjojen kanssa sovelletaan ensisijaisesti muita kuin tätä liitettä, sopimuksessa kuvatulla tavalla.

Kansalaishavainnot

Kansalaishavainnoilla tarkoitetaan tietoa, joka on ilmoitettu yleiseen käyttöön havaitsijan omasta aloitteesta tai havaitsijan itsenäisellä päätöksellä. Kansalaishavaintotietoja ei siis ole tuotettu työ-, virka-, konsultti- tai muun sopimuksen puitteissa, eikä niiden toimittaminen tietojen kerääjälle muodosta tällaista sopimusta tai suhdetta. SYKE kerää kansalaishavaintoja sekä toimialaansa kuuluvista määrittelemistään aiheista joko

1. Mittauksenkaltaisina havaintoina ympäristön tilasta (”**havaintoja**”)
2. Tietoina tapahtumista, ilmiöistä, suunnitelmista tai päätöksistä (”**ilmoituksia**”) tai
3. Ilmoituksia näin tai muuten tuotettujen tietoaineistojen laadusta, laatupoikkeamien tai ilmiöiden edellyttämistä toimenpiteistä sekä tällaiseen havaintotoimintaan tai sen ohjaukseen kuuluvista muista tiedoista tai tiedonannoista (näihin kaikkiin muihin kuin havaintoihin ja ilmoituksiin viitataan käsitteillä ”**annotaatio**”, ”**annotaatiohavainnot**” ja ”**annotaatioilmoitukset**”).

Kansalaishavaintojärjestelmään ja joukkoistamisjärjestelmiin liittyvät määrittelyt

1. **CitobsDB**llä tarkoitetaan SYKE:n ylläpitämää tietojärjestelmää, jolla tuotetaan internet –yhteyden avulla käytettäviä tiedon kuvailu-, rakenteen-määrittely-, tallennus-, haku- ja lataustoimintojen palveluita.
    a. CitobsDB päätarkoitus on kansalaishavaintojen kerääminen kansalais-havaintojen ilmoittajilta (”**ilmoittaja**” tai ”**havaitsija**”). lisäksi järjestelmässä on kerättävän tiedon määrittelyn, palveluiden ja oikeuksien hallinnan sekä tiedon avoimen käytön hallinnan toimintoja.
    b. CitobsDB tarjoaa koneluettavia rajapintapalveluita verkkosivuilla toimiville havaintoilmoitusten verkkolomakkeille ja muille palveluille, erityisesti ennaltamääriteltyjä kysymyspattereita käyttöohjeineen erilaisia havaintotilanteita ja ilmoituksia varten. Rajapintapalvelua käyttävät muut järjestelmät esittävät kysymykset ja ohjeet käyttäjilleen ja tallentavat näiden perusteella muodostetut kansalaishavainnot CitobsDB järjestelmään. Tallennettuja kansalaishavaintotietoja voidaan hakea saman rajapinnan avulla muiden järjestelmien käyttöön.
    c. **’Ilmoituspalvelulla’** tarkoitetaan kansalaishavaintojärjestelmässä olevaa jokaiselle kansalaishavaintoaiheelle tehtyä omaa palvelua, joka määrittelee aiheesta kerättävän tiedon sisällön, vastaanottaa siitä tehdyt ilmoitukset ja palauttaa joukkoistamisjärjestelmälle ilmoituspalveluun tallennetut kansalaishavaintotiedot määriteltyjen hakuehtojen perusteella. Jokaisella ilmoituspalvelulla on palvelun kautta kerättävän tiedon tietomallin version yksilöivä palvelutunnuskoodi (**service code**). Jokaisella ilmoituspalvelun kautta ilmoitetun arvonsa tallennettavalla ilmoituspalvelun kysymyspatterin kysymyksellä eli attribuutilla on oma attribuuttitunnuksensa (**code**).
    d. **’Kansalaishavaintotiedolla’** tarkoitetaan tietoa, joka syötetään kansalaishavaintojärjestelmään joukkoistamisjärjestelmien avulla. Yksittäinen kansalaishavaintotieto voidaan kansalaishavaintojärjestelmässä merkitä avoimeksi tai suljetuksi. Kansalaishavaintotieto koostuu määritellystä ryhmästä atribuutteja ja niiden tietosisältöjä. Yksittäinen joukkoistamisjärjestelmässä ilmoitettu ja sen avulla tietyn ilmoituspalvelun kautta kansalaishavaintojärjestelmään tallennettu kansalaishavaintotieto voidaan yksilöidä sen yksilöllisen havainto-ID –tunnuksen avulla.

2. CitobsDB ja sen toimintojen avulla toteutetut käytännöt ilmoitusten vastaanottamiseksi, käsittelemiseksi, tallentamiseksi ja jakelemiseksi SYKE palveluissa ja avoimen tiedon rajapinnoissa muodostavat SYKEn ylläpitämän **kansalaishavaintojärjestelmän**, jonka avulla SYKE tarjoaa **kansalaishavaintopalveluita**.
3. Kansalaishavaintojärjestelmää toiminnassaan käyttävät järjestelmät ovat **joukkoistamisjärjestelmiä**.
    a. Tyypillisesti ne joukkoistamispalveluidensa avulla keräävät kansalaishavaintotietoa käyttäjiltään esimerkiksi verkko-sivujensa tai mobiilipalveluidensa toiminnan osana, ja toimittavat sitä edelleen kansalaishavaintojärjestelmään tallennettavaksi ja tämän joukkoistamispalveluille yhteisen kansalaishavaintotietovarannon kautta yhteisesti jaeltavaksi tiedoksi.
4. **Joukkoistamispalvelut** koostuvat paitsi teknisistä järjestelyistä havainto-tietojen lähettämiseksi kansalaishavaintojärjestelmään, myös erilaisista muista tehtävistä (”ei-teknisistä järjestelyistä”), joita niihin saatetaan sisällyttää:
    a. Havaitsijoiden rekrytointi ja kouluttaminen
    b. Tiedottamisen, sidosryhmäviestintä ja mainonta
    c. Erilaisten havaintotapahtumien, toimintakampanjoiden, kilpailujen ja vastaavien järjestäminen
    d. Tavoitteiden ja muiden säännöllisen tai urakkaluonteisen havaintotoiminnan tai tiedonkeräyksen puitteiden sopiminen havaitsijoiden ja heidän yhteisöjensä kanssa
    e. Havaintoaineistojen laadunvarmistuksen menettelyt
    f. Havaintotoiminnan ohjaus erityisesti tiedon kattavuuden ja havaintojen riittävyyden varmistamiseksi
    g. Muut joukkoistamispalveluihin liittyvät toimet joita joukkoistamispalvelun ylläpitäjä toimintaan päättää sisällyttää

SYKEn kansalaishavaintotoiminnan yhteydessä käytetyt käsitteet

1. Tarjottujen CitobsDB:n koneluettavien rajapintojen, tietoaineistojen, neuvonnan, havaintojärjestelyiden ja järjestelmäkehityspalveluiden kokonaisuuteen viitataan termillä ”**SYKEn kansalaishavaintopalvelut**”.
2. Tiedon kerääminen kansalaishavaintopalveluihin CitobsDB järjestelmään tapahtuu joko SYKEn omien verkko- tai mobiilipalveluiden (”**SYKE:n joukkoistuspalvelut**”) tai muiden toimijoiden kansa-laishavaintoja keräävien, hyödyntävien ja SYKE:lle CitobsDB järjestelmään välittävien palveluiden (”**joukkoistuspalvelut**” tai ”**ulkoiset joukkoistuspalvelut**”) kautta.
3. Kansalaishavaintojen havaitsijat ja muut tiedon ilmoittajat ovat joukkoistamispalveluiden asiakkaita
4. Joukkoistamispalvelut ja niitä toteuttavat järjestelmät SYKEssä tai SYKEn ulkopuolella puolestaan ovat kansalaishavaintojärjestelmän asiakkaita ja asiakasjärjestelmiä.

API-avaimet ja -avaintunnukset

API-avaimella tarkoitetaan koneluettavan rajapinnan käytön yhteydessä joukkoistuspalvelun tai muun järjestelmän kansalaishavaintopalvelulle ilmoittamaa merkkijonoa, jolla tietoja syöttävä tai suljettua tietoa lukeva palvelu (tyypillisesti joukkoistamispalvelu) tunnistautuu ja ilmaisee käyttöoikeuden toimittamaansa tai käyttämäänsä kansalaishavaintotietoon.

Yksittäinen, vaihdettavissa oleva API-avaimen kooditieto (tietty satunnaisesti valittujen numeroiden, kirjainten ja muiden merkkien jono) liittyy **API-avaintunnukseen**, jolle on määritelty käyttötarkoitus esimerkiksi tietyissä joukkoistamisjärjestelmissä ja vastuuhenkilö yhteystietoineen.

1. API-avaintunnus **luodaan** CitobsDB järjestelmässä, kun sille määritellään avaintunnukseen liittyvät yhteystiedot. Luomisen yhteydessä API-avain syntyy automaattisesti
2. API-avaintunnukseen syntynyt avain voidaan **regeneroida** eli luoda uusi satunnaismerkkien merkkijono. Aiemmin käytössä ollutta merkkijonoa ei voida palauttaa takaisin käyttöön, eikä regeneroidun merkkijonon sisältöä voida määritellä, ohjata tai muokata. API-avain on siis vain tunniste, joka sinänsä ei voi sisältää informaatiota. Kahden samanlaisen merkkijonon syntyminen on äärimmäisen epätodennäköistä, niin että sitä voidaan pitää käytännössä mahdottomana.

3. API-avaintunnukseen liittyvä API-avain voidaan myös ottaa pois käytöstä (”**deaktivoida**”) tai deaktivointi purkaa (jäljempänä ”**aktivoida**”): Deaktivoidulla API-avaimella kaikki uuden tiedon syöttäminen ja kyseiseen API-avaintunnukseen liitetyt mahdollisuudet päästä käsiksi muuhun kuin yleisesti saatavilla olevaan tietoon on estetty.

CitobsDB järjestelmässä olevat yksittäisinä kansalaishavaintoina ilmoitetut tiedot voivat olla **avointa** tai **suljettua tietoa** eli avoimesti kaikkien käyttäjien CitobsDB järjestelmän rajapinnoista luettavissa ja haettavissa olevia tietoja tai vain suljetulle erikseen käsittelyyn oikeutetulle ryhmälle saatavissa. Oman API-avaimensa avulla kansalaishavaintojärjestelmään tietoa syöttävä voi rajapinnasta hakea myös suljetussa tilassa olevat kansalaishavaintoilmoituksensa saman API-avaimen avulla, mutta ei muita suljetussa tilassa olevia tietoja.

SYKEssä CitobsDB järjestelmän ylläpidon hallussa on ”**Master API-avain**”, jonka avulla voidaan tarkastella kaikkien toimijoiden tallentamaa suljettua tietoa sekä myöntää luottamuksellisesti säilytettäviä CitobsDB järjestelmässä määriteltyjä joukkoistamisjärjestelmiä varten API-avaintunnuksia ja niihin liittyviä API-avaimia.

”API-avaimenhaltija” ja ”API-yhdyshenkilö”

1. Joukkoistamisjärjestelmä joka itse tallentaa tietoja kansalaishavaintojärjestelmään tarvitsee oman API-avaintunnuksen. Tällaisesta joukkoistamisjärjestelmästä vastaava SYKE ulkopuolinen organisaatio tai SYKEn työryhmä, palvelu tms. on ”**API-avaimenhaltija**”.
2. API-avaimia toimitetaan API-avaimenhaltijoina asiaan kuuluvien toimijoiden yhdyshenkilöille, jotka vastaavat organisaatiossaan käytännön asianmukaisista toimista niiden käyttämiseksi (”**API-yhdyshenkilö**”).

API-avaintunnukset määritellään nimeämällä kahteen luokkaan sen mukaan, onko niiden käsittelyssä noudatettava maltillisia vai huomattavan varovaisia tietoturvakäytäntöjä: I-API-avaimeen yhdistyvät avaintunnukset ovat tyypillisesti käytössä verkkosivuilla, ja TL-API-avaimia käytetään palvelinten väliseen tiedonsiirtoon. Kansalaishavaintojärjestelmästä voidaan nopeasti, tarvittaessa ilman ennakkoilmoitusta deaktivoida API-avaimen oikeudet mikäli sen kautta toimitetaan merkittävästi ilmeisen asiatonta dataa esimerkiksi häirintätarkoituksessa. Tässä suhteessa I-API-avain ja TL-API-avain (ja vastaavat API-avaintunnukset) eivät poikkea toisistaan.

’TL-API-avaimella’ tarkoitetaan API-avainta, joka on tarkoitettu palvelinten väliseen ja muuten vahvasti suojattuun ja salattuun tiedonvaihtoon.

1. Turvaluokitellusti säilytettävä API-avain eli jäljempänä ”**TL-API-avain**”: API-avain jonka on tarkoitettu lähinnä palvelinten väliseen ja muuten vahvasti suojattuun ja salattuun tiedonvaihtoon.
2. Lähtökohtaisesti riski että TL-API-avain päätyy muiden kuin joukkoistamisjärjestelmän ja SYKE kansalaishavaintojärjestelmän ylläpitohenkilökunnan tietoon sitoudutaan molemminpuolisesti minimoimaan.
3. TL API-avainta voidaan tyypillisesti käyttää joukkoistamisjärjestelmän tietokannasta tehtäviin siirtoihin keskitetysti suoraan kansalaishavaintojärjestelmään.
    a. Verkkosivuille asennetuissa widgeteissä ja erilaisista mobiililaitteisiin asennetuista sovelluksista API-avaimen haltuunotto saattaa olla mahdollista riippumatta joukkoistamisjärjestelmän haltijan ja muiden omista tai vaikutusvallassa olevista toimenpiteistä, joten joukkoistamistelmälle annetaan vähintään yksi tavallinen, tietoturvaltaan mahdollisesti vaarantuneisiin paikkoihin tarkoitettu I-API-avain, joka on tarkoitettu nopeasti vaihdettavaksi mikäli käy ilmi, että se on joutunut vääriin käsiin.
    b. TL-API-avaimen ei pitäisi koskaan päätyä esim verkkosivujen kautta saataville, joten sen voidaan olettaa olevan turvallisemmassa tallessa kuin esimerkiksi widgeteissä käytetty I-API-avain.
    c. TL-API-avaimen vaihtaminen palvelimelta vaatii tyypillisesti muutakin kuin tavalliset editointioikeudet verkkosivuille, joten deaktivointi voi aiheuttaa joukkoistamisjärjestelmän ylläpidolle hankalamman tilanteen.
4. Joukkoistamisjärjestelmän sisäisissä tiedonsiirroissa ei näin käytetä TL-API-avainta, vaan muita tunnistamismenettelyitä, joten TL-API-avainta ei tietona kopioidu esimerkiksi mobiilipäätelaitteisiin tehtyihin joukkoistamisjärjestelmän asennuksiin.

5. Pääsääntöisesti yhdelle joukkoistamisjärjestelmälle myönnetään **vain yksi** TL-API-avaintunnus, johon liittyy yksi aktivoitu tai deaktivoitu TK-API-avain.

'I-API-avaimella' tarkoitetaan ns. tavallista API-avainta, jota voidaan käyttää esimerkiksi joukkoistamisjärjestelmien käyttäjille latautuvilla verkkosivuilla tai heille jaettavissa mobiiliaplikaatioissa.

1. Verkkosivu-, mobiilipäätelaite- ja internetkäyttöön tarkoitettu API-avain on **tavallinen API-avain** ja sopimusteksteissä myös "**I-API-avain**" kun on tarpeen korostaa eroa TK-API-avaimen kanssa
2. Verkkosivuille asennetuissa widgeteissä ja erilaisista mobiililaitteisiin asennetuista sovelluksista API-avaimen haltuunotto saattaa olla mahdollista riippumatta joukkoistamisjärjestelmän haltijan ja muiden omista tai vaikutusvallassa olevista toimenpiteistä, joten joukkoistamistelmälle annetaan vähintään yksi tavallinen, tietoturvaltaan mahdollisesti vaarantuneisiin paikkoihin tarkoitettu API-avain, joka on tarkoitettu nopeasti vaihdettavaksi mikäli käy ilmi, että se on joutunut vääriin käsiin
3. Vain tavallista API-avainta eli I-API-avainta saa käyttää osana Citobs Open311 Widget –koodia verkkosivuilla tai mobiilipäätelaitteeseen asennetun ohjelmiston osana, mukaan lukien laitteen muistiin kopioitu tieto.
4. API-avaimen yhteyshenkilö voi kansalaishavaintopalveluiden ylläpidon kanssa erikseen sovittavalla tavalla luovuttaa I-API-avaimen oman organisaationsa henkilöstöön kuuluvalle tai muulle yhteistyökumppanille esimerkiksi ylläpitotoimenpiteitä varten. Luonnollisesti näiden henkilöiden on noudatettava API-avaimen käsittelystä annettuja tietoturva- ja muita ohjeita.
5. Samalle joukkoistamisjärjestelmälle voidaan myöntää useita I-API-avaintunnuksia joihin jokaiseen liittyy yksi aktivoitu tai deaktivoitu I-API-avain.
6. I-API-avain on tarkoitettu pääasiallisesti käytettäväksi API-avaimeksi kansalais-havaintopalveluiden kanssa käytävässä yhteydenpidossa kaikissa muissa paitsi valtuusavaimiin ja kuratoinnin toimeenpanoon liittyvään annotaatioon liittyvissä toimenpiteissä. Niissäkin I-API-avaimen käyttö on mahdollista, kunhan toimiin liittyvät riskit ja niiden toteutumisen aiheuttamien vahinkojen vaikutukset arvioidaan huolellisesti.

API-avaimen avulla, sen ilmoittamalla valtuudella, joukkoistamisjärjestelmä siirtää asiakkaansa eli havaitsijan tuottaman kansalaishavaintoilmoituksen SYKE:n kansalaishavaintojärjestelmään jonne se tallennetaan kansalaishavaintojärjestelmän toiminnan ajaksi lähtökohtaisesti pysyvästi ja pääsääntöisesti toimituksen yhteydessä määritellyllä tavalla yleisiltä käyttöoikeuksiltaan avoimeksi tai suljetuksi.

API-yhdyshenkilöille määritellään joukkoistamisjärjestelmäänsä varten tyypillisesti vähintään kaksi API-avaintunnusta. "API-avaintunnuksen" tietoihin kuuluu API-yhteyshenkilön nimen ja käytettävissä olevien yhteystietojen (sähköposti ja puhelinnumero) lisäksi "**API-avaintunnuksen nimi**", joka kuvaa API-avaintunnuksen käyttötarkoitusta ja siihen liittyvää joukkoistamisjärjestelmää sekä "**API-avaintunnuksen kuvaus**" jossa lyhyellä tekstillä viitataan ja kuvataan API-avaimen käyttötarkoitus, sekä varsinainen API-avain. API-avaimen kirjain- ja numerosarjaa voidaan vaihtaa ja se voidaan deaktivoida API-avaintunnuksen määrittelemän yhteyden pysyessä voimassa.

CitobsDB järjestelmän kehittyessä API-avaintunnukseen liitetään myös tietoja kyseisen tunnuksen muista käyttöoikeuksista CitobsDB järjestelmän toimintoihin, esimerkiksi oikeudesta merkitä nimettyjen ilmoituspalveluiden tietoja suljetuiksi tai avoimiksi.

API-avaintunnuksen nimen pohjana on tyypillisesti **joukkoistamisjärjestelmän nimi**, johon on eri tavoin lisätty käyttötapatietoja, esimerkiksi TL –alkuisia API-avaintunnusten nimiä käytetään TL-API-avaintunnusten yhteydessä. **Joukkoistamisjärjestelmän kuvausta** käytetään tyypillisesti pohjana kun täsmennetään joukkoistamisjärjestelmän tietyn API-avaintunnuksen kuvaustietoja. Nämä joukkoistamisjärjestelmän ylläpitäjältä sopimuksen määrittelyiden yhteydessä tulleet tiedot ovat kansalaishavaintojärjestelmän API-avaintunnustietojen määrittelyn pohjana.

API-avainten käyttö

Aktivoidulla API-avaimella tarkoitetaan API-avainta jonka oikeudet syöttää tietoa CitobsDB järjestelmään ja lukea sille oikeutettuja kansalaishavaintoilmoituksia. **Deaktivoidulla** API-avaimella kaikki uuden tiedon syöttäminen on estetty. Kansalaishavaintojärjestelmä voi automaattisesti tai sen

ylläpitohenkilökunta erillisin toimenpitein ja rajauksin voi poistaa syötetyn tiedon tai estää pääsyn tai tiedonsyöttöoikeuden eri API-avainten avulla eri tyyppisiin kansalaishavaintoilmoituksiin. Kansalaishavaintojärjestelmän ylläpito voi aktivoida tai deaktivoida API-avaimen sekä muuttaa ja asettaa uusia rajauksia ja oikeuksia API-avaimille ilman erillistä ilmoitusta myös sopimuksen solmimisen jälkeen ja koskien jo aiemmin syötettyä tietoa.

Ylläpitohenkilökunnalla viitataan tietoteknistä järjestelmien ja palveluiden ylläpitotyötä suorittavaan henkilöstöön joko kansalaishavaintojärjestelmän ylläpito-henkilökuntaan SYKE:ssä tai SYKE:n kanssa näitä toimia sopimussuhteessa toteuttavissa organisaatioissa; tai joukkoistamisjärjestelmän ylläpitohenkilökun-taan API-avaimenhaltijan omassa tai sen kanssa näitä toimia koskevassa so-pimussuhteessa toteuttavissa organisaatioihin. SYKE:n yhteyshenkilönä järjestelyistä toimii kansalaishavaintojärjestelmän pääkäyttäjä (”**kansalaishavaintovastaava**”).

- SYKE ulkopuolisen API-avaimenhaltijan API-yhdyshenkilö vastaa joukkoistamisjärjestelmän osalta ylläpitohenkilökunnan sopimuksenmukaisista järjestelyistä.

Kansalaishavaintojärjestelmän tekniset toteutuspalvelut joukkoistamisjärjestel-mille

Citobs Open311 Widget (jäljempänä myös ”**widget**”) on internet-yhteydellä toimivalle verkkosivustolle asennettava käskyjono (jäljempänä ”widget-koodi”), joka sisältäessään aktivoidun API-avaimen voi tuot-taa verkkoselaimessa tietyn aiheen kansalaishavaintoilmoituslomakkeen uusien tietojen lähettämistä varten (”**ilmoituswidget**”).

- Ilman API-avainta voidaan widgetin avulla verkkosivulle luoda kansa-laishavaintojen verkkokartan, joka avulla voi tarkastella avoimeksi mer-kittyjä kansalaishavaintotietoja (”**karttawidget**”).
- Widgetit, kuten kansalaishavaintojärjestelmän tekniset toteutuspalvelut joukkoistamisjärjestelmille lähtökohtaisesti muutenkin, syöttävät havaitsijan tuottaman havainnon suoraan kansalaishavaintojärjestelmään. Näin joukkoistamisjärjestelmään ei jää erillistä kopiota syötetystä tiedosta, eikä joukkoistamisjärjestelmältä voida edellyttää havaintotiedon ennakkotarkastamista ennen kansalaishavaintojärjestelmään syöttämistä.

Kansalaishavaintokampanjat (jäljempänä myös ”**kampanjat**”) viittaavat tietyn aihepiirin joukkoistetut tietojen hankinnan ja käsittelyn kokonaisuuteen: Yhden tai useamman toisiinsa liittyvän ilmoituspalvelun tietojen keräämisen ja analysoinnin käytännön järjestelyt ja ohjeistus, havainnoinnin ja muun osallistumisen organisointi, viestintä ja toiminnan tulosten hyödyntäminen. Kampanjalla on tyypillisesti joukkoistetun tiedonhankinnan lisäksi myös muita tavoitteita, kuten esimerkiksi yleisen tietoisuuden nostaminen aihepiirin kysymyksistä, kansalaisten päätöksentekoon osallistumisen tukeminen, ympäristön kunnostustoimenpiteiden valmistelu ja suorittaminen tai osallistumismahdollisuuksien luominen ympäristön seurantaan ja tieteelliseen työhön sekä tätä koskevaan viestintään.

Kansalaishavainnot.fi palvelu on SYKE kansalaishavaintopalvelun ylläpi-tämä havaintokampanja-alusta, joka on toteutettu SYKE verkkosivujen teemasivustona. Havaintokampanja-alusta tarjoaa paikan paitsi valmiiksi asennetuille kartta- ja ilmoituswidgeteille, myös verkkosivujen kokonai-suuden kampanjakohtaisen ohjeistuksen ja muun havaintotoiminnan järjestelytiedon julkaisemiselle sekä esimerkiksi palveluiden tiedontuoton tavoitteille tai viestintämateriaalin jakelulle.

Jatkossa kansalaishavaintojärjestelmän tarjoamia toteutuspalveluita saatetaan laajentaa muillakin palveluilla. Näissä saattaa olla myös joukkoistamisjärjestelmälle toimitettavan tiedon käsittelymahdollisuus suoraan kansalaishavaintojärjestelmään tallentamisen lisäksi.

Ilman aktivoitua API-avainta tai deaktivoidun API-avaimen sisäl-tävän widget –koodin (karttawidgetin) avulla on mahdollista esittää verkkosivulla avoimiksi merkittyjä havaintoja kyseisestä aiheesta kartalla sekä aiheen ilmoituslomakkeen kysymysrakenteen ohjeineen ja kysymyskohtaisine vaihtoehtoineen, mutta ilman kansalaishavainnon lähetysmahdollisuutta.

Antamalla widget-koodin sisältävälle verkkosivulle käyttöoikeuden paikannustietoon, voi karttanäkymän kohdistaa paikannustiedon mukaisesti. Widgetin toiminta edellyttää mahdollisuutta ja oikeutusta käynnistää verkkosivulta SYKE hallitsemille palvelimille asennettu palvelinohjelma kyseisen selainnäkymän tuottamiseksi.

Kansalaishavaintotiedoista

CitobsDB:n mukautetussa ja laajennetussa Open311 rajapintapalvelussa jokaiselle kansalaishavaintoaiheelle on oma palvelunsa (”**ilmoituspalvelu**” tai ”**service**”), joka tunnistetaan palvelun tunnuksella (”**service code**”, tai myös ”**palvelu-ID**” eli ”**ServiceID**”).

Näihin palveluihin syötetty yksittäinen havainto-, ilmoitus- tai annotaatio-tieto muodostaa aina yhden havainnon, joka tunnistetaan havainnon identifikaationumerolla (”**service request ID**”, jäljempänä myös ”**havainto-ID**” eli ”**ObservationID**”).

Kansalaishavaintotieto eli havaintotieto koostuu ryhmästä palvelussa ennalta määriteltyjä kysymyksiä (”**attribuutti**” tai ”**muuttuja**”) ja niihin havainnossa mahdollisesti annettuja vastauksia (”**attribuuttitieto**”). Yksittäiseen kysymysmuotoiluun eli attribuuttiin viitataan kysymyksen tunnuksella (jäljempänä myös ”**attribuutin tunnus**” eli ”**code**”). i. Kansalaishavaintojärjestelmä saa jakaa sille toimitettuja ja tallennettuja tietoja Creative Commons 0 -tahdonilmauksen mukaisesti.

Kansalaishavaintojärjestelmän ylläpito tai kansalaishavaintojärjestelmään liitetty automaatio voi poistaa avoimen tiedon aineistosta näkyvistä avoimena tietona toimitetun havainnon, kopioida toimitetun havainnon ja tallentaa sen uudelleen korjattuna, antaa vapaasti annotoida kerättyä havaintotietoa annotointiin määriteltyjen palveluiden avulla sekä yhdistellä ja julkaista näistä tiedoista uusia tietotuotteita ja kansalaishavaintoja.

Avoimen eli julkisen ja suljetun eli luottamuksellisen kansalaishavaintotiedon aineistot ja rajapinnat

CitobsDB palvelussa on kaksi joukkoistamisjärjestelmien käyttöön tarkoitettua koneluettavaa rajapintaa

1. **Laajennettu Open311 –rajapinta**, jonka kautta voidaan paitsi tal-lentaa myös hakea tietyn ilmoituspalvelun kautta ilmoitettuja kansalaishavaintoja. Aktiivisen API-avaimen avulla tunnistautu-minen oikeuttaa lukemaan myös samalla API-avaintunnuksella tallennettuja suljetuiksi merkittyjä kansalaishavaintoja. Avoimia tietoja ja ilmoituspalveluiden kuvauksia voi lukea myös ilman tunnistautumista.
2. Kansalaishavaintojen **avoin paikkatietorajapinta**, jonka kautta voi ilman tunnistautumista lukea avoimia kansalaishavaintotietoja. Suljettuja kansalaishavaintotietoja ei voi tarkastella kansalaishavaintojen avoimesta rajapinnasta lainkaan.

Suljetuiksi eli luottamuksellisiksi CitobsDB palveluun tallennetaan tai merkitään jälkikäteen ne ne tallennetut havainnot, joita ei erilaisista syistä johtuen haluta antaa yleiseen vapaaseen avoimeen käyttöön ilman käyttörajoitteita.

Avoimeksi eli julkiseksi merkityt kansalaishavaintotiedot ovat automaattisesti saatavilla kansalaishavaintojen avoimesta paikkatietorajapinnasta ilman merkittäviä käyttörajoitteita. Avoimen kansalaishavaintotiedon käyttöoikeuksissa määritellään käytetty avoimen tiedon lisenssi.

Avoimen tiedon suljetuksi merkitseminen poistaa kansalaishavaintotiedon automaattisesti kansalaishavaintojen avoimesta paikkatietorajapinnasta, ja uudelleen avoimeksi merkitseminen palauttaa sen kyseiseen jakeluun. Avoimeksi tai suljetuksi merkitsemisen päätös- ja toimeenpanoprosessia kutsutaan **kuratoimiseksi**, ja sen yhteydessä voidaan myös harkita uusien ilmoituspalveluiden tarvetta ja vanhojen ilmoituspalveluiden toiminnan tai ohjeistuksen muuttamista.

Avoimeksi merkityt havainnot julkaistaan erikseen paikkatietorajapinta-aineistona yleisesti tuetuilla tekniikoilla karttajärjestelmien jne käyttöön. Yksittäinen kansalaishavaintotieto merkitään avoi-meksi eli julkiseksi mikäli ei ole erillistä syytä olla julkaisematta sitä tai erikseen poistaa sitä julkisen havaintotiedon aineistosta. Suljetuksi merkittyjä havaintoja ei avoimeen paikkatietorajapinta-aineistoon kuulu, vaan ne on luettavissa vain laajennetusta Open311 rajapinnasta lukemiseen oikeuttavan API-avaimen avulla.

Kuratoinnin yhteydessä kansalaishavaintojen ylläpito mahdollisuuksien mukaan varmistaa, että jo kerätyt havaintoaineistot tai niihin tehdyt annotaatiot ja muut laadunvarmistustoimenpiteet säilyvät käyttökelpoisina siten, että kerättävän aineiston laadun voidaan kuratointitoimenpiteiden johdosta katsoa nousseen.

Tietojen poisto avoimesta jakelusta eli sulkeminen, suljetun tiedon käyttöoikeu-det sekä tietojen ylikirjoittaminen eli poistaminen

Kuratoimisen yhteydessä aiemmin avoimena jaetun yksittäisen kansalaishavaintotiedon merkitseminen suljetuksi eli avoimesta jakelusta sulkeminen poistaa kyseisen tiedon avoimena jaettavan tiedon aineistosta ja alistaa sen suljetulle tiedolle asetetuille käyttörajoituksille.

Joukkoistamisjärjestelmä pääsee, järjestelmän käyttämän API-avaimen valtuuksien perusteella, käsiksi erilaisiin kansalaishavaintojärjestelmässä suljetuiksi merkittyihin tietoihin. Näitä koskevat erityisesti seuraavat rajoitukset

1. Yleiset suljetun kansalaishavaintotiedon käyttöoikeuden rajoitukset
    a. Katso sopimusteksti liitteineen ja asianomaiset käyttöoikeuslisenssit
    b. Yleisesti ottaen suljettua tietoa ei saa levittää joukkoistamisjärjestelmän käyttäjille ilman eri lupaa
2. Kansalaishavaintojärjestelmän suljetuiksi merkittyjen joukkoistamisjärjestelmän itse toimittamien tietojen käyttöoikeus
    a. Katso sopimusteksti liitteineen ja asianomaiset käyttöoikeuslisenssit
    b. Yleisesti joukoistamisjärjestelmä saa hyödyntää toiminnassaan itse tallentamaansa suljettua tietoa
3. Kansalaishavaintojärjestelmän suljetun annotaatiotiedon käyttöoikeus
    a. Katso sopimusteksti liitteineen ja asianomaiset käyttöoikeuslisenssit
    b. Yleisesti suljetuissa annotaatioissa on myös joukkoistamisjärjestelmien tarvitsemia ohjeita. Tyypillisesti tietosisällöstä ilmenee tai on muuten ilmeistä missä laajuudessa joukkoistamisjärjestelmän oletetaan paljastavan ko tietoja käyttäjälleen. Joukkoistamisjärjestelmien ei pidä paljastaa näitäkään suljettuja tietoja laajemmin kuin asianmukaisen tiedon käsittelytoiminnan järjestämiseksi on välttämätöntä.

Kansalaishavaintojärjestelmän suljetun annotaatiotiedon pääsääntöinen käyttöohjeistus: Lähtökohtaisesti joukkoistamisjärjestelmä ei saa paljastaa käyttäjilleen tai välittää eteenpäin kansalaishavainto-järjestelmästä saamansa suljetun tiedon sisältöä. Joukkoistamisjärjestelmä kuitenkin saa automaattissa toiminnoissaan hyödyntää myös suljettuna annotaationa avoimeen tietoon merkittyjä tietoja (”**suljettua annotaatiotietoa**”) ja itse kansalaishavaintojärjestelmään syöttämiään tietoja (”**suljetuiksi merkityt omat havainnot**”) kunhan asianmukaisesta tietosuojasta huolehditaan.

Erityisesti joukkoistamisjärjestelmässä on huolehdittava että virheellisinä tai asiattomina ilmoituksina, tai tietosuojasyistä suljetuiksi merkittyjä tietoja ei julkistettaessa liitetä avoimeen tietoon tai muuten asiattomasti julkisteta tai aiheuteta sekaannuksen vaaraa käyttökelpoisen tiedon kanssa.

Suljetun kansalaishavaintotiedon käyttöoikeuksista voi kansalaishavaintojärjestelmä ohjeistaa erikseen joukkoistamisjärjestelmä- ja ilmoituspalvelukohtaisesti. Kansalaishavaintojärjestelmän ylläpito saa antaa suljetun annotaatiotiedon käyttöä koskevia velvoittavia ohjeita niille joukkoistamisjärjestelmille, jotka käyttävät näissä ”**suljetun annotaatiotiedon käyttöohjeissa**” nimettyjä annotaatioiden ilmoituspalveluita.

1. Tietosuojakäytäntöjensä mukaisella prosessilla kansalaishavaintojen ylläpito voi ylikirjoittaa eli lopullisesti poistaa kansalaishavaintojärjestelmään toimitettuja tietoja attribuuttitietokohtaisesti tai kokonaisuudessaan.
    a. Ylikirjoitetut alkuperäiset tiedot on ensin suljettu avoimesta käytöstä, ja ylikirjoittamisen jälkeen kaikki joukkoistusjärjestelmien oikeudet alkuperäiseen kansalaishavaintojärjestelmässä tallennettuna olleeseen tietoon lakkaavat, eli alkuperäinen tieto on jaosta poistettava ja tuhottava.
2. Alkuperäisen attribuuttitiedon tekstin päälle kirjoitettava uusi teksti tai tekstin poistava tyhjä merkkijono saattavat poistaa alkuperäisen tiedon tietosuojaongelman, joten ilmoituksen muu sisältö saattaa muutetun sisältönsä vuoksi olla avoimena julkaistavissa niinkutsuttuna **uudelleenkirjoitettuna havaintona** samalla havainto-ID tiedolla.

Lähtökohtaisesti kansalaishavaintojärjestelmässä ei avata julkiseen käyttöön uudelleenkirjoitettuja havaintoja. Välttämättä avoin annotaatiotietokaan ei tässä yhteydessä tekisi riittävän selvää eroa käyttäjille saman havainto-ID avulla haetuista alkuperäisistä ja myöhemmin ylikirjoitetuista tietosisällöistä. Osittaisen ylikirjoittamisen avulla syntyneet uudelleenkirjoitetut havainnot pidetään tyypillisesti suljettuna tietona. Tässä käytäntö voi ilmoituspalvelukohtaisesti vaihdella.

Yksilöivä havainto-ID on käytössä myös ylikirjoitetun tiedon tapauksessa: Samaa havainto-ID tietoa ei koskaan käytetä uuden riippumattoman havaintotapauksen tiedon tallentamiseen, mutta aiempaan havainto-ID tietoon voidaan annotoida uusi, korvaava tieto, jolla on oma havainto-ID.

Tyypillisessä virheellisten ilmoitusten korjaustavassa virheellinen ilmoitus merkitään suljetuksi, se annotoidaan virheen kuvauksella ja viittauksella uuteen, erillisenä saman ilmoituspalvelun havaintona tallennettuun havaintoon, jota kutsutaan **korvaavaksi havainnoksi**.

Lähtökohtaisesti useimmissa tapauksissa kuratoinnissa riittää joko havaintotiedon sulkeminen tai korvaava havainto, ja ylikirjoittaminen on erikseen perusteltava poikkeus.

Kansalaishavaintopalveluiden ylläpito voi merkitä avoimena CitobsDB järjestelmässä julkaistun tiedon suljetuksi, jolloin se poistuu avoimena julkaistun tiedon aineistosta. Suljetut tiedot ovat vain kansalasihavaintojärjestelmän sisäisessä käytössä tai ne API-avaimellaan toimittaneen joukkoistamisjärjestelmän käytössä. Kansalaishavainto-palveluiden ylläpito poistaa vuosittain tai erillisillä päätöksillä erikseen havainto-ID ja attribuuttikohtaisesti yksilöityjä suljettujen havaintotapausten tietoja myös joukkoistamisjärjestelmien ja kansalaishavaintojärjestelmän käytöstä ylikirjoittamalla tai muuten lopullisesti poistamalla niiden tietosisällöt tietokannasta. Näin poistettu tieto poistuu ja tuhoutuu myös suljetuista kansalaishavainnoinnin tietoaineistoista.

Erillisellä sopimuksella voidaan yhdessä sopia ”suljetun kansalaishavaintotiedon käyttöoikeuksista”, joukkoistamisjärjestelmä- ja ilmoituspalvelu-kohtaisesti.

Joukkoistamisjärjestelmät eivät saa välittää käyttäjilleen kansalaishavaintojärjestelmän suljetuiksi merkittyjä tieto-ja, ellei tästä ole erikseen joukkoistamisjärjestelmä- ja palvelukohtaisesti sovittu.

Henkilötiedot, anonyymit tiedot ja pseudonymisointi

Anonyymillä tiedolla tarkoitetaan kansalaishavaintojärjestelmässä kaikkia niitä havaintotietoja joiden havainnontekijää ei voida tiedosta yksilöidä.

Kansalaishavaintojärjestelmä on lähtökohtaisesti anonyymin tiedon tietojärjestelmä, eli se ei kerää havaitsijoiden henkilötietoja tai tunnista havaitsijoita tai havaintojen lähettäjiä. Myöskään tieto avoimen havainnon lähettäneestä joukkoistusjärjestelmästä ei ole avoimesti saatavilla.

Pseudonymisoidulla tiedolla tarkoitetaan anonyymejä havaintoja, joihin on lisätty attribuuttitietona **pseudonymisointikoodi**. Joukkoistusjärjestelmäkohtaisen, hankekohtaisen jne.

pseudonymisointikoodien tulkintalistan eli **koodiavaimen** avulla henkilötietojen haltija voi yhdistää pseudonymisointikoodin henkilötietoihin ja tämän kautta mahdollisesti yksilöityyn havaintotiedon toimittajan henkilöön.

Joukkoistamisjärjestelmän vastuu pseudonymisointikoodeista:
Muille käyttäjille havaintotiedon on pysyttävä anonyymina pseudonymisointikoodin merkkijonosisällön avoimuudesta huolimatta, koska se yksin ei saa olla yhdistettävissä henkilöön ilman koodiavainta. Kansalaishavaintojärjestelmässä ei saa käyttää helposti saatavista lähteistä peräisin olevia koodiavaimia pseudonymisointiin.

Anonyymillä tiedolla tarkoitetaan kansalaishavaintojärjestelmässä kaikkia niitä havaintotietoja joiden havainnontekijää ei voida tiedosta yksilöidä.

CitobsDB järjestelmä ei lähtökohtaisesti tallenna sille Open311 spesifikaation (www.open311.org) kautta tallennuksessa tarjottuja tietoja, joten ellei henkilötietoja erikseen lisätä havaintotiedon osaksi tieto on anonyymiä.

Lähtökohtaisesti henkilötietojen kirjaaminen mihin tahansa kansalaishavaintojärjestelmän attribuuttiin, joka vastaanottaa tekstiä tai merkkijonoja syötteeksi, on kielletty.

Kansalaishavaintojärjestelmän ylläpito ei salli henkilötietoja keräävien kyselyiden käyttöä kansalaishavaintojärjestelmässä. Kansalaishavaintojärjestelmän ylläpito sulkee avoimesta jakelusta pois henkilötietoja sisältävät havaintoilmoitukset.

Pseudonymisoidulla tiedolla tarkoitetaan anonyymejä havaintoja, joihin on lisätty attribuuttitietona pseudonymisointikoodi. Joukkoistusjärjestelmäkohtaisen, hankekohtaisen jne. pseudonymisointikoodien tulkintalistan eli koodiavaimen avulla henkilötietojen haltija voi yhdistää pseudonymisointikoodin henkilötietoihin ja tämän kautta mahdollisesti yksilöityyn havaintotiedon toimittajan henkilöön. Muille käyttäjille havaintotiedon on pysyttävä anonyymina pseudonymisointikoodin merkkijonosisällön avoimuudesta huolimatta, koska se yksin ei saa olla yhdistettävissä henkilöön ilman koodiavainta. Tällaista pseudonymisoitua tietoa voidaan tallentaa kansalaishavaintojärjestelmään mikäli koodiavaimien henkilötietoihin yhdistävien tietojen ja pseudonymisointitietoa hyödyntävän havaintojen keräyksen tietosuo-javelvoitteista on asianmukaisesti huolehdittu joukkoistamisjärjestelmän ylläpitäjän puolesta myös kansalaishavaintojärjestelmän ylläpidolle ilmoitetulla tavalla.

Käyttövaltuuskooditiedot

Käyttövaltuuskoodilla tarkoitetaan kansalaishavaintojärjestelmässä havaintotiedon yhteydessä attribuutinarvona esiintyvää merkkijonoa, joka havaintotiedon osana tiedonkäsittelyjärjestelyissä erikseen sovitun attribuutin arvona kertoo joukkoistamisjärjestelmän puolesta kansalaishavaintojärjestelmälle, että tallennettu havainto- tai ilmoitustieto saa käynnistää toimenpiteen kansalaishavainto-järjestelmässä. Esimerkkinä toimenpiteestä tietyn attribuutin arvona olevan havainto-ID:n viittauksen ja toisen attribuutin mukana tulevan valinnan mukaan tämä viitattu havaintotieto voidaan muuttaa avoimeksi tai suljetuksi.

Kansalaishavaintojärjestelmä ja viime kädessä sen ylläpito päättää toteutetaanko kansalaishavaintojärjestelmässä kyseinen toimenpide.

Käyttövaltuuskoodi voi toimia itsenäisesti toistuvasti tai kertakäyttöisesti, tai vain yhdessä tiettyjen pseudonymisointikoodien, havainto-id tai palvelu-id arvojen tai muiden ehtojen kanssa joukkoistamisjärjestelmän ja kansalaishavaintojärjestelmän ylläpitojen kesken sovitulla tavalla.

Käyttövaltuuskoodeja on mahdollista liittää kansalaishavaintojärjestelmään kerättäviin tietoihin, mutta ne eivät saa sisältää viittauksia henkilö-tietoihin eikä niiden liittämiselle avoimesti jaettaviin aineistoihin saa olla rajoituksia.