Tarkastusraportti tietoturvamerkkiä varten - RuuviTag

1 Johdanto ja tarkastuksen johtopäätökset

Ruuvi Innovations on hakenut RuuviTag-laitteelle ja siihen liittyvälle älypuhelinsovellukselle Liikenne- ja viestintäviraston Kyberturvallisuuskeskuksen tietoturvamerkkiä. Tässä raportissa kuvataan Kyberturvallisuuskeskuksen tuoteturvallisuustoiminnon niistä tekemät havainnot ja johtopäätökset.

RuuviTag-laite on pieni paristokäyttöinen sääasema, joka mittaa lämpötilaa, kosteutta, ilmanpainetta ja omaa asentoaan. Mitatut tiedot laite lähettää langattomasti Bluetooth Low Energy (BLE) -yhteyden avulla Ruuvi Station -älypuhelinsovellukselle. RuuviTag ja siihen liittyvät sovellukset on toteutettu avoimena lähdekoodina - kaikki lähdekoodit ovat vapaasti saatavilla. Koska RuuviTag on avoin ja sitä on mahdollista käyttää myös muutoin, on se saavuttanut suuren käyttäjäjoukon erityisesti tekniikan alan harrastajien parissa.

Laitteen ja siihen liittyvän älypuhelinsovelluksen tarkastus on suoritettu uhkamallinnuksessa tunnistettuja uhkia vastaan. Viitekehyksinä on käytetty Kyberturvallisuuskeskuksen tietoturvamerkin vaatimuksia, jotka pohjautuvat ETSI standardiin TS 303 645. Tarkastuksen aikana arvioitiin myös yleisesti tietoturvamerkin soveltuvuutta lyhyen kantaman radiolaitteille ja näihin sovellettavia vaatimuksia.

RuuviTag ei käytä tietojen lähetyksessä tietojen salausta. Tämän johdosta kuka tahansa laitteen kantomatkan sisällä voi vastaanottaa ja tarkastella laitteen lähettämiä tietoja. Tietoturvamerkin yleisenä tarkoituksena on osoittaa, että laite ja sen käyttäjä ovat turvassa internetistä tulevia uhkia vastaan. Merkin vaatimuksiin kuuluu mm. turvallinen viestintä. RuuviTagin tapauksessa on katsottu, että pelkkä salaamaton lyhyen kantaman radioliikenne ei uhkaa laitteen tai sen käyttäjän turvallisuutta etenkin kun huomioon otetaan lähetettävän tiedon sisältö ja luonne.

Liikenne- ja viestintäviraston Kyberturvallisuuskeskuksen tuoteturvallisuustoiminto ei ole suorittamassaan tarkastuksessa havainnut sellaisia puutteita, mitkä olisivat esteenä tietoturvamerkin myöntämiselle. Tehtyjen havaintojen mukaan RuuviTagille ja siihen olennaisesti liittyvälle Ruuvi Station -sovellukselle voidaan myöntää tietoturvamerkki.

2 Tarkastus

2.1 Tarkastuksen kohde ja menetelmät

Tietoturvamerkkiin tähtäävän tarkastuksen kohteena olivat:

- RuuviTag, laiteohjelmistoversio 2.5.9
- Ruuvi Station -Android-sovellus, versio 1.1.9
- Ruuvi Station -iPhone-sovellus, versio 0.6

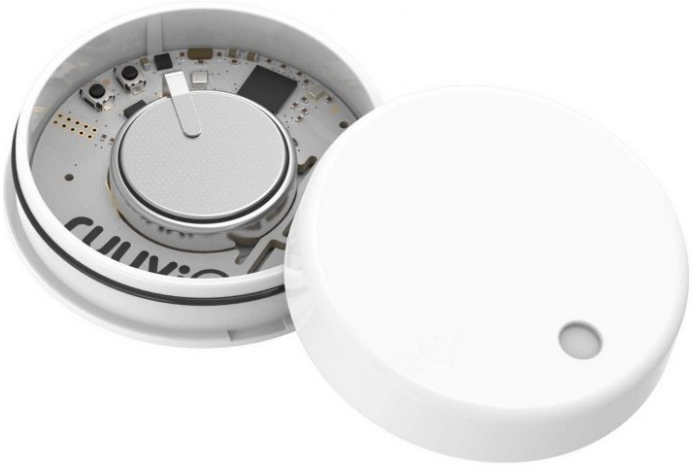
Tarkastus suoritettiin tarkastelemalla RuuviTagin ja Ruuvi Station -mobiilisovelluksen toimintaa eri tilanteissa, testaamalla käytännössä eri hyökkäysskenaarioita, analysoimalla lähdekoodia ja keskustelemalla kehittäjien kanssa eri komponenttien ominaisuuksista ja toiminnasta. RuuvinTagin avoimuudesta johtuvat käyttötapaukset, jotka pohjautuvat muihin laiteohjelmistoihin tai sovelluksiin, ei ole sisällytetty tehdyn tarkastuksen piiriin.

Mobiilisovelluksen osalta tekninen tarkastus on suoritettu pääasiassa Android-sovellukselle ja sen tulokset on yleistetty käsittämään myös iPhone-sovellus. Sellaisten ominaisuuksien osalta, mitkä ovat vain iPhone -sovelluksessa, tarkastus on pohjautunut sovelluksen lähdekoodin tarkasteluun.

Ruuvi Innovations on tuomassa markkinoille myös RuuviTagin uudella laiteohjelmistolla (versio 3) sekä Ruuvi Gateway -yhdyskäytävätuotteen. Nämä eivät ole nyt tehdyn tarkastuksen piirissä, vaan mahdollisesti tarkastetaan erikseen myöhempänä ajankohtana.

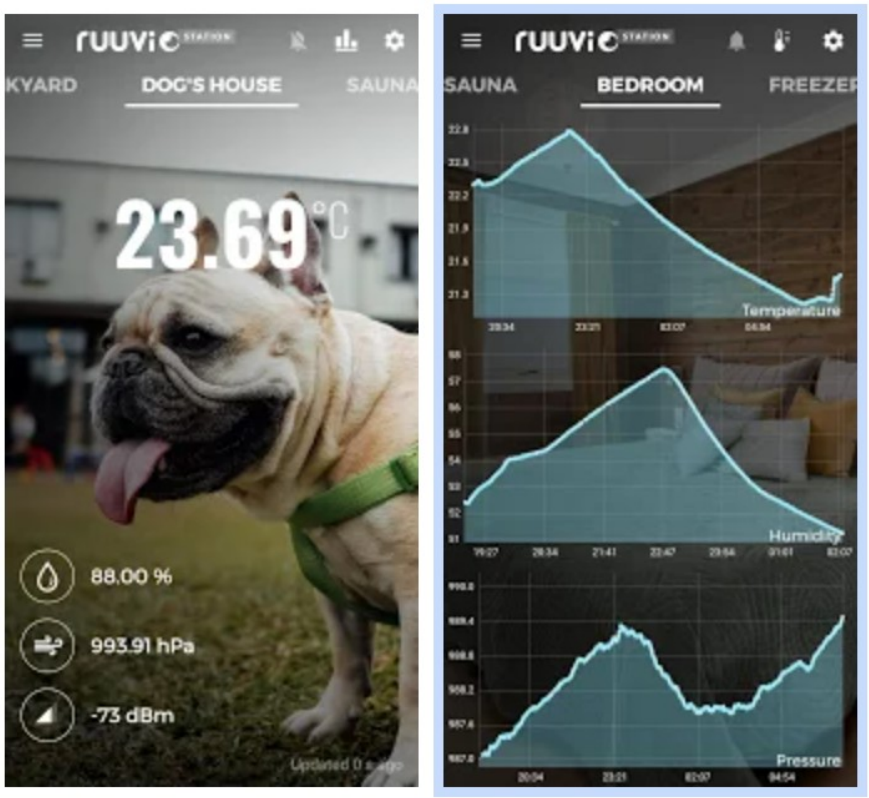
2.2 Järjestelmän toiminta

RuuviTag sisältää useita antureita, jotka mittaavat ympäristöstä lämpötilaa, ilmankosteutta ja ilmanpainetta. Lisäksi laite mittaa oman asentonsa ja pariston jännitteen. Mitatut suureet RuuviTag lähettää säännöllisesti radioteitse käyttämällä Bluetooth Low Energy (BLE) -teknologiaa. Lähetys on ns. mainostus, mikä on kaikkien lähialueella olevien BLE-laitteiden vastaanotettavissa. RuuviTagissa on lisäksi tuki ns. NFC-yhteyskäytännölle. NFC-lukijan avulla on mahdollista lukea laitteen tunnistetiedot ja laiteohjelmiston versionumero. RuuviTag sen kotelo avattuna on esitetty seuraavassa kuvassa. Halkaisijaltaan laite on n. 52 mm.



RuuviTagin sisällä olevalla painikkeella on mahdollista vaihtaa tietojenlähetyksen aikaväliä tai vaikuttaa mainostuksen tietojen muotoon. Laitteen painikkeita tarvitaan myös tilanteessa, jossa laiteohjelmisto halutaan päivittää uudempaan versioon käyttämällä älypuhelinta.

Ruuvi Station -älypuhelinsovelluksella RuuviTagin käyttäjä voi tarkastella laitteen keräämiä tuloksia ja näistä piirrettyjä kuvaajia. Halutessaan käyttäjä voi määrittää sovelluksen välittämään kerätyt tiedot edelleen kolmannen osapuolen palveluun. Applen IOS -alustalla oleva sovellus tukee lisäksi ns. virtuaalisia antureita, joiden avulla sovellus voi esittää käyttöliittymässä eri kaupunkien yleisiä säätietoja. IOS-sovellus tukee myös RuuviTageihin suunniteltua ominaisuutta, jossa älypuhelin voi pyytää RuuviTagilta sen mittaushistoriaa. Tämä historiatiedon siirto tulee RuuviTagin laiteohjelmistoversiossa 3, mikä ei ole nyt tehdyn tarkastuksen piirissä. Ruuvi Station -sovelluksen tyypilliset näkymät on esitetty seuraavassa kuvassa:



RuuviTagin toiminnassa olennaista on, että sen käyttö ei vaadi esimerkiksi salasanoja tai erillisen pariliitoksen muodostamista älypuhelimeen. Kaikki kantomatkan sisällä olevat laitteet voivat vastaanottaa mitattuja tietoja.

2.3 Uhkamalli

Tietoturvamerkin myöntämiseen tähtäävän tietoturvatarkastuksen pohjana on uhkamalli, mihin sisältyvät seuraavassa esitetyt uhat. Näiden osalta on arvioitu hyökkäysten toteutuksen vaatimia resursseja ja käyttäjälle tästä kohdistuvaa uhkaa. Lisäksi on arvioitu sitä, mitkä uhista ovat tietoturvamerkin vaatimusten piirissä ottaen huomioon RuuviTagin ominaisen toimintatavan ja lähettävien tietojen luonteen.

- Mobiililaitteen sisäinen hyökkäys ilman pääkäyttäjäoikeuksia
  - Käyttäjän lataama ohjelma pyrkii vaikuttamaan sovelluksen toimintaan tai keräämään tietoja.
    - Testattu, ei mahdollista.

- Välimieshyökkäys verkkoliikenteelle
  - Mobiililaite on kytketty wifi-verkkoon tai muutoin internetissä oleva taho pyrkii keräämään tai muuttamaan sovelluksen käyttämiä tietoja verkkoliikennettä käsittelemällä.
    - Testattu, lähtökohtaisesti ei mahdollista.
      Mikäli käyttäjä erikseen ottaa käyttöön Ruuvi Stationin Gateway-toiminnallisuuden ja määrittelee sen siten, että salaamatonta https-yhteyskäytäntöä ei käytetä, on tietojen lähetys ulkoiseen palveluun altis välimieshyökkäykselle.

- Hyökkäys internetistä mobiililaitetta vastaan
  - Internetistä pyritään vaikuttamaan suoraan sovellukseen tai sen toimintaan.
    - Testattu, ei mahdollista.

- RuuviTagiin vaikuttaminen etäältä
  - RuuviTagin toimintaan vaikutetaan BLE-yhteyden kautta.
    - Testattu, ei mahdollista. Ei vaatimusten piirissä.
      RuuviTag laiteohjelmistoversio 2 ei ota vastaan lähetyksiä. Ohjelmiston yleistä kypsyyttä arvioitiin saapuvan tiedon käsittelyn avulla käyttämällä laiteohjelmistoversiota 3, mikä ei ole nyt tehdyn tarkastuksen piirissä.

- RuuviTagin lähettämien tietojen kuuntelu
  - Ulkopuolinen taho kuuntelee RuuviTagin lähettämiä tietoja.
    - Testattu, mahdollista. Ei vaatimusten piirissä.
      Käyttäjään kohdistuvaa uhkaa rajaa RuuviTagin lähetysten rajallinen kantomatka ja lähetettävän tiedon sisältö.

- RuuviTagin lähettämien tietojen väärentäminen
  - Ulkopuolinen taho pyrkii lähettämään väärennettyjä datapaketteja RuuviTagin nimissä.
    - Testattu, mahdollista. Ei vaatimusten piirissä.
      Uhkaa rajaa BLE-lähetysten rajallinen kantomatka. Lisäksi tämän suoritus vaatii syvällistä teknistä osaamista.

- RuuviTagin lähetysten estäminen
  - Ulkopuolinen taho pyrkii estämään RuuviTagien käytön tietyllä alueella radiohäirinnän avulla.
    - Mahdollista. Ei vaatimusten piirissä.

2.4 Vaatimustenmukaisuusilmoitus

Ruuvi Innovationsin Kyberturvallisuuskeskukselle 25.9.2020 toimittama tietoturvamerkin vaatimustenmukaisuusilmoitus on vastaanotettu ja käsitelty, eikä tässä ole havaittu puutteita.

Vaatimustenmukaisuusilmoituksessa on ilmoitettu lukuisten vaatimusten osalta, että vaatimus ei sovellus RuuviTagin kohdalla. RuuviTagin tapauksessa voidaan katsoa, että järjestelmässä ei ole sensitiivisiä tietoturvaan vaikuttavia parametreja, eikä ole tarvetta viestiä tietoturvallisesti laitteen toiminnot ja lähettävän tiedon sisältö huomioon ottaen.

Mikäli Ruuvi Innovations niin katsoo esim. teknisten liikesalaisuuksien johdosta, on tietoturvamerkki.fi -verkkosivustolla mahdollista julkaista lomakkeesta sisällöltään rajoitetumpi versio.

2.5 Android käyttöjärjestelmän sisäiset rajapinnat ja sovelluksen oikeudet

Android-käyttöjärjestelmä tarjoaa laitteen sisäisiä rajapintoja, minkä avulla sovellukset voivat kommunikoida keskenään eri tavoin. Sovelluksen käyttämät rajapinnat tarkastettiin eikä niissä havaittu sellaisia puutteita, mitkä altistaisivat käyttäjän tiedot muiden sovellusten käytettäväksi. Android-laitteella sovellus vaatii seuraavat käyttöoikeudet:

- BLUETOOTH
- BLUETOOTH_ADMIN
- ACCESS_COARSE_LOCATION
- ACCESS_FINE_LOCATION
- INTERNET
- WAKE_LOCK
- FOREGROUND_SERVICE
- RECEIVE_BOOT_COMPLETED

Sovelluksen vaatimia käyttöoikeuksia ei havaittu tarpeettoman laajoiksi sovelluksen käyttöskenaariot huomioiden tai muutoin uhkaavan käyttäjän tietoturvaa.

2.6 Käyttäjän tietojen kerääminen ja säilytys

Sovellus tallentaa älypuhelimeen ainoastaan lyhytaikaista historiatietoja RuuviTageilta kerätyistä tiedoista. Nämä tiedot ovat kenen tahansa vastaanotettavissa RuuviTagin kantomatkan sisällä. Käyttäjän yksilöiviä tietoja ei kerätä.

2.7 API-rajapinnat ja verkkotekninen tarkastus

Käytettäessä sovellusta vain RuuviTagien tietojen lukemiseen ja esittämiseen ei sovellus käytä ulkoisia rajapintoja. Mikäli iPhone-sovelluksessa otetaan käyttöön virtuaaliset anturit, hakee sovellus tietoja OpenWeatherMap-palvelun API-rajapinnasta. Jos sovelluksessa otetaan käyttöön ns. Gateway-palvelu, lähettää sovellus tiedot käyttäjän määrittelemään API-rajapintaan. Molemmissa tapauksissa sovellus viestii HTTP(S)-yhteyskäytännöllä. Sovelluksen kypsyyttä saapuvan tiedon käsittelyn osalta arvioitiin tarjoamalla sen lähettämiin pyyntöihin epäkelpoja vastauksia. Puutteita ei havaittu.

RuuviTagin tarkastuksen piirissä ollut laiteohjelmistoversio ei vastaanota mitään tietoja. Jotta laitteen verkkoteknisten ominaisuuksien yleistä kypsyyttä voitiin arvioida, päivitettiin yksi laite ns. beta-asteella olevaan laiteohjelmistoversioon 3, missä on ominaisuus tietojen vastaanotolle BLE-yhteyden kautta. Tietoja vastaanottavaa RuuviTagia arvioitiin lähettämällä sille suuri määrä epäkelpoa liikennettä, eli ns. fuzz-testauksen avulla. Puutteita ei havaittu laitteen toiminnassa tai vastaanotettujen tietojen käsittelyssä.

2.8 Mittaustietojen lähetyksen tietoturvasta

RuuviTag lähettää mittaustiedot ilman salausta. Näin ollen kuka tahansa laitteen kantomatkan sisällä voi vastaanottaa laitteen lähettämiä tietoja. Tiedon lähetyksessä ei ole myöskään käytössä tietojen allekirjoitusta, joten tietojen alkuperästä tai eheydestä ei voi olla täyttä varmuutta.

RuuviTagin suorittaman mittauksen ja tietojen lähetyksen taajuus on suhteellisen matala (~0,5 Hz). Mikäli anturi on sijoitettuna esimerkiksi suihkutiloihin tai jääkaappiin, on sen lähettämästä tiedosta suhteellisen helppoa päätellä tapahtumia. Muissa tiloissa tiedoista päätelmien tekeminen on merkittävästi vaikeampaa. Vaikeusastetta päätelmien tekoon lisää huomattavasti se, että yksittäisen RuuviTagin tarkkaa paikkaa on haastavaa päätellä ilman asianmukaista osaamista ja välineitä. Myös hyökkäyksen etäisyyttä rajaa tehokkaasti RuuviTagin radiosignaalin kantama.

Koska RuuviTagin lähettämässä datapaketissa ei ole käytössä allekirjoitusta on teknisesti mahdollista lähettää valeliikennettä, joka vaikuttaisi tulevan RuuviTagista. Tällaisen väärennetyn liikenteen lähettäminen vaatii hyvää teknistä osaamista, siihen soveltuvia laitteita ja asiaan vihkiytymistä. Lisäksi hyökkäyksen vaikeusastetta nostaa hyökkäyksen mahdollinen kantomatka. Vaikka hyökkäys toteutetaan, voi sillä enintään vaikuttaa yhden käyttäjän älypuhelimen esittämiin tietoihin lämpötilasta ja muista suureista.

Käytännössä mahdollisen hyökkäyksen RuuviTagin käyttäjää vastaan on oltava kohdennettu. Tällaisen hyökkäyksen tapauksessa RuuviTag ei todennäköisesti paljasta sellaisia seikkoja, mitkä eivät muin keinoin olisi saatavilla selville kohtuullisella vaivalla. Myöskään käyttäjään ei väärennetyillä tiedoilla voi vaikuttaa niin, että siitä olisi vähäistä suurempaa haittaa. RuuviTag ei altista käyttäjää internetistä tuleville uhille tai mahdollista ns. massahyökkäyksiä. Näin ollen tietojen salaamattomuutta tai allekirjoituksen puutetta ei ole katsota ongelmaksi tässä käyttötapauksessa tietoturvamerkin kontekstissa.

2.9 Tietoturvamerkin vaatimukset

Tässä kappaleessa esitetään vaatimukset tietoturvamerkin puolesta ja tarkastuksessa tehdyt havainnot kunkin vaatimuksen osalta. Kunkin vaatimuksen ohessa on viittaus standardin ETSI TS 303 645 kohtaan.

- Where passwords are used and in any state other than the factory default, all consumer IoT device passwords shall be unique per device or defined by the user (ETSI 5.1-1).
    - Järjestelmässä ei käytä salasanoja.

- The manufacturer shall make a vulnerability disclosure policy publicly available (ETSI 5.2-1).
    - Ruuvi Innovations ei ole julkaissut varsinaista käytäntöä haavoittuvuuksien raportointiin. Yritys on kuitenkin helposti saavutettavissa kaikissa sen laitteisiin liittyvissä asioissa ja kysymyksissä. Tuoteperheen laajuus ja ominaisuuksien luonne huomioon ottaen tämä katsotaan riittäväksi.

- Manufacturers should continually monitor for, identify and rectify security vulnerabilities within products and services they sell, produce, have produced and services they operate during the defined support period (ETSI 5.2-3).
    - Ilmoituksensa ja keskustelujen perusteella Ruuvi Innovations seuraa tuotteissaan olevia haavoittuvuuksia.

- When the device is not a constrained device, it shall have an update mechanism for the secure installation of updates (ETSI 5.3-2).
    - RuuviTag ja Ruuvi Station ovat päivitettävissä.

- An update shall be simple for the user to apply (ETSI 5.3-3).
    - RuuviTagin laiteohjelmiston päivitys on ohjeistettu siten, että kuka tahansa ilman syvällistä teknistä osaamista voi päivittää laiteohjelmiston. Ruuvi Station -sovellus päivitetään sovelluskaupan kautta.

- Updates shall be timely (ETSI 5.3-8).
    - RuuviTagin päivitysvälistä ei ole olemassa sellaista historiatietoa, mistä voi tehdä päätelmiä. Ottaen huomioon laitteen toiminnot ja käsittelemät tiedot, sekä yrityksen sitoutumisen laitteen kehittämiseen, tätä ei pidetä puutteena.

- The manufacturer should inform the user in a recognizable and apparent manner that a security update is required together with information on the risks mitigated by that update (ETSI 5.3-11).
    - Ilmoituksensa perusteella Ruuvi Innovations tiedottaa tuotteitaan koskevasta päivitystarpeesta.

- The manufacturer shall publish, in an accessible way that is clear and transparent to the user, the defined support period (ETSI 5.3-13).
    - Tukiaika on määritelty. 25.9.2020 saadun tiedon mukaan tuen kesto on voimassa vuoden 2025 loppuun.

- Sensitive security parameters in persistent storage shall be stored securely by the device (ETSI 5.4-1).
    - Tuotteessa ei ole tietoturvaan vaikuttavia parametreja.

- The consumer IoT device shall use best practice cryptography to communicate securely (ETSI 5.5-1).
    - RuuviTagin tapauksessa on katsottu, että salaamaton BLE-mainostus ei vaaranna käyttäjän tietoturvaa kun huomioidaan lähettävän tiedon sisältö ja tekninen toteutus.

- Device functionality that allows security-relevant changes in configuration via a network interface shall only be accessible after authentication (ETSI 5.5-5).
    - Tuotteen asetuksiin ei voi tehdä muutoksia verkkorajapintojen kautta. RuuviTagin laiteohjelmistopäivitys vaatii fyysisen painikkeen painamista.

- The manufacturer shall follow secure management processes for critical security parameters that relate to the device (ETSI 5.5-8).
    - Tuotteessa ei ole tietoturvaan vaikuttavia parametreja.
- All unused network and logical interfaces shall be disabled (ETSI 5.6-1).
    - Tuotteissa ei ole ylimääräisiä verkkorajapintoja.
- Software should run with least necessary privileges, taking account of both security and functionality (ETSI 5.6-7).
    - Vaatimus täyttyy tehtyjen havaintojen perusteella.
- Installation and maintenance of consumer IoT should involve minimal decisions by the user and should follow security best practice on usability (ETSI 5.12-1).
    - RuuviTagin käyttöönotto on suoraviivaista, eikä siinä vaadita päätöksentekoa.
- The manufacturer should provide users with guidance on how to securely set up their device (ETSI 5.12-2).
    - RuuviTagin käyttöönotossa ei ole tietoturvaan vaikuttavia parametreja, joten ohjeistusta turvallisesta käyttöönotosta ei edellytetä.
- The consumer IoT device software shall validate data input via user interfaces or transferred via Application Programming Interfaces (APIs) or between networks in services and devices (ETSI 5.13-1).
    - Testattu käytännössä, vaatimus täyttyy.
- The manufacturer shall provide consumers with clear and transparent information about what personal data is processed, how it is being used, by whom, and for what purposes, for each device and service. This also applies to third parties that can be involved, including advertisers (ETSI 6.1).
    - Järjestelmä itsessään ei kerää tai käsittele henkilötietoja. Analytiikan osalta tiedot on anonymisoitu. Käytännöt henkilötietojen käsittelyyn on kuvattu asianmukaisesti.