TRAFICOM
Kyberturvallisuuskeskus

17.11.2020

Tietoturvamerkin vaatimustenmukaisuuslomake

Lomakkeen käyttö

Tämä lomake tarjoaa tietoa IoT-tuotteen tietoturvallisuudesta kansalliselle tietoturvaviranomaiselle sekä teknisesti orientoituneille kuluttajille. Lomake julkaistaan osana tietopakettia kuluttajille aina, kun uusi Tietoturvamerkki myönnetään.

Osio 1 tarjoaa yleistä tietoa merkin saaneesta tuotteesta ja siihen liittyvästä ekosysteemistä, kuten mobiilisovelluksista ja kolmannen osapuolen tarjoamista pilvipalveluista. Osio 2 käsittelee kuluttajien kannalta merkityksellisiä tietoturvauhkia sekä niiden torjumiseen käytettäviä tietoturvallisuusvaatimuksia. Vaatimuskohtien yhteyteen on liitetty taulukoita, joita voi käyttää apuna lomakkeen täyttämisessä silloin, kun se on mahdollista ja järkevää. Lomakkeessa annetaan myös esimerkkejä tavoista, joilla tuotteen tietoturvallisuusominaisuuksia voidaan kuvata.

Tämän tekstin viittaukset ETSIin ovat vaatimuksia, jotka esitetään standardissa ETSI EN 303 645 "CYBER; Cyber Security for Consumer Internet of Things". Standardi saatavilla osoitteessa https://www.etsi.org/deliver/etsi_en/303600_303699/303645/02.01.01_60/en_303645v020101p.pdf

Yhteystiedot

Yrityksen nimi:	DNA Oyj
Y-tunnus	0592509-6

1 Tuotekuvaus

Kuvaa tuote tai tuoteperhe (Tuote), jolle merkkiä haetaan. Kuvaa myös valmistajan tai Tuotteen toiminnan kannalta olennainen kolmansien osapuolten tarjoama ekosysteemi (Palvelu).

DNA Oyj:n Wattinen on älylämmityspalvelu kaukolämmitteisten asunto-osakeyhtiöiden kiinteistöihin. Palvelukokonaisuus sisältää älytermostaatin per lämpöpatteri ja usean termostaatin jakaman yhdyskäytävälaitteen yleisiin tiloihin (yhdessä Tuote) sekä taustajärjestelmän ja mobiilisovelluksen loppukäyttäjälle (yhdessä Palvelu). Asunto-osakeyhtiölain 22.12.2009/1599 2 §:n mukaan lämmitysjärjestelmä kuuluu taloyhtiön vastuulle. Asunto-osakeyhtiön päätöksellä Wattinen asennetaan kattamaan kiinteistön koko lämmitysjärjestelmä. Asunto-osakeyhtiö tekee DNA Oyj:n kanssa jatkuvan kuukausilaskutussopimuksen, joka takaa Wattisen ylläpidon sopimuksen keston ajaksi.

1.1 Tuen kesto

Valmistajan tulee ilmaista käyttäjälle selvällä ja läpinäkyvällä tavalla Tuotteelle taattava tukijakso (ETSI 5.3-13). Määrittele tukijakso ja kerro, kuinka siihen liittyvä tieto on käyttäjän saatavilla.

Tuote ja Palvelu ovat tietoturvapäivitysten piirissä DNA Oyj:n ja asunto-osakeyhtiön välisen sopimuksen keston ajan.

1.2 Tietoturvaohjeistus

Valmistajan tulee tarjota käyttäjille ohjeet Tuotteen turvalliseen käyttöönottoon (ETSI 5.12-2). Kerro, missä tietoturvaohjeistus on saatavilla suomeksi.

Loppukäyttäjä ei osallistu Tuotteen asennukseen tai huoltoon, vaan ne kuuluvat DNA Oyj:n ja asunto-osakeyhtiön välisen sopimukseen. Wattisen älytermostaatit ja yhdyskäytävälaitteet asennetaan asunto-osakeyhtiön tiloihin DNA Oyj:n tarjoaman ammattilaisen toimesta. Palvelun suomenkieliset ohjeet: https://www.wattinen.fi/tietopankki

1.3 Muut sertifikaatit ja merkit

Kuvaa muut sertifikaatit, joiden vaatimukset Tuote täyttää. Esimerkiksi CE-merkki ja/tai FCC-merkki; Tuotteella on sertifikaatti X (esim. UK:n tietoturvamerkki, lisää linkki); taho Y on todentanut tuotteessa käytetyt palvelukomponentit

Tuote on CE-merkitty. Tuotteella tai Palvelulla ei ole ulkopuolisen palveluntarjoajan tietoturvasertifikaattia.

2 Suojautuminen tyypillisiä IoT-uhkia vastaan

Tuote on suojattu tyypillisiltä IoT-uhilta seuraavissa osioissa kuvatuilla tavoilla.

2.1 Heikot, helposti arvattavat tai kovakoodatut salasanat

Salasanoja koskeva vaatimustaso on kuvattu seuraavassa. Osoita kunkin vaatimuksen toteutuminen käyttäen tarkastuslistaa.

	Vaatimustenmukainen	Ei sovellu	Ei tietoa	Vaatimus ei täyty
Tuotteen salasanojen täytyy aina olla yksilöllisiä ja laitekohtaisia tai käyttäjän itsensä määrittelemiä, jos Tuote ei ole tehdasasetustilassa (ETSI 5.1-1).	☒	☐	☐	☐

Kuvaa miten Tuote on suojattu heikkojen tai kovakoodattujen salasanojen muodostamalta uhalta. Kuvaa, miten vahvoja ja yksilöllisiä salasanoja vastaava tietoturvallisuustaso on saavutettu. Esimerkkinä: jos tuote on esimerkiksi suojattu muutoin kuin käyttäjän tunnistusta hyödyntäen tai jos käyttäjän tunnistaminen tapahtuu muutoin kuin salasanan avulla.

Tuotteet ovat DNA Oyj:n ja asunto-osakeyhtiön sopimuksen keston ajan yhteydessä vain DNA Oyj:n ylläpitämän virtuaalisen yksityisverkon sisällä oleviin Palvelun komponentteihin yksityisen APN-verkon avulla. Tuotteessa ei ole geneerisiä tai kovakoodattuja salasanoja. Tuotteen käyttöliittymä loppukäyttäjälle on kaksitasoinen:

1) Fyysinen pääsy Tuotteelle ja lämpötilan säätö perinteisen termostaatin tavoin.
2) Mobiilisovellus, jossa tunnistautuminen toteutetaan SMS-viestillä lähetettävällä kertakäyttösalasanalla. Loppukäyttäjähallinnassa hyödynnetään Amazon Cognito -palvelun tietoturvasertifioituja ominaisuuksia.

2.2 Turvattomien tai vanhentuneiden komponenttien käyttö

Turvattomien tai vanhentuneiden komponenttien käyttöä koskevat vaatimukset ovat seuraavat. Osoita kunkin vaatimuksen toteutuminen käyttäen tarkastuslistaa.

	Vaatimustenmukainen	Ei sovellu	Ei tietoa	Vaatimus ei täyty
Muiden kuin hyvin kapasiteetiltaan hyvin rajallisten laitteiden tulee sisältää turvallisen päivityksen mahdollistava päivitysmekanismi (ETSI 5.3-2).	☒	☐	☐	☐
Päivitysten asentamisen pitää olla käyttäjälle yksinkertaista (ETSI 5.3-3).	☒	☐	☐	☐
Päivitykset on toimitettava kohtuullisessa ajassa (ETSI 5.3-8).	☒	☐	☐	☐
Valmistajan tulee kertoa käyttäjälle selkeästi ja ymmärrettävästi vaadittavista tietoturvapäivityksistä sekä riskeistä, joilta päivitykset suojaavat (ETSI 5.3-11).	☒	☐	☐	☐

Valmistajan tulee asettaa haavoittuvuuksien hallintapolitiikkansa julkisesti saataville (ETSI 5.2-1).	☒	☐	☐	☐
Valmistajan tulee jatkuvasti havainnoida, tunnistaa ja poistaa tietoturvallisuuteen liittyviä haavoittuvuuksia tuotteissa ja palveluissa, joita se myy, tuottaa tai on tuottanut (ETSI 5.2-3).	☒	☐	☐	☐

Kuvaile kuinka Tuote tai Palvelu on suojattu turvattomien ja vanhentuneiden komponenttien aiheuttamalta uhalta. Kuvaa esimerkiksi, miten kaikkien komponenttien haavoittuvuuksia seurataan alihankintaketjuissa, mukaan lukien käyttöjärjestelmät, verkkopalvelut sekä ohjelmistokirjastot. Kuvaa, miten oikea-aikaisuus, asennuksen helppous, laadunvarmistus ja turvallinen tiedonsiirto ja asennus on varmistettu Tuotteen päivityksessä. Päivitysväli vaihtelee tyypillisesti 30–90 päivän välillä, mutta tämä voi vaihdella merkittävästi tuotetyypeittäin.

DNA Oyj:llä on tiedossaan jokaisen asennetun Tuotteen fyysisten ja ohjelmistokomponenttien versiot. DNA Oyj:n ja asunto-osakeyhtiön välisen sopimuksen voimassaoloaikana DNA Oyj:n edustajat monitoroivat käytössä olevia Tuotteita jatkuvasti Palvelun komponenttien avulla. Tuotteiden ohjelmistoja päivitetään ajoittain myös etänä.
Jos Tuotteissa havaitaan tietoturvahaavoittuvaisuuksia tai muita ongelmia, DNA Oyj vaihtaa Tuotteet uusiin sopimuksen mukaisesti. Lisäksi DNA Oyj vaihtaa ajoittain vanhentuneita Tuotteita proaktiivisesti Palvelun vaatimusten mukaisesti.

Palvelun kaikki ohjelmistokomponentit sijaitsevat DNA Oyj:n ylläpitämässä pilvi-infrastruktuurissa virtuaalisessa yksityisverkossa. Virtuaalinen yksityisverkko kattaa myös yhteyden Tuotteisiin yksityisen APN-verkon avulla.

Palvelun komponentteja päivitetään 7-14 päivän syklissä jatkuvan integraation ja jatkuvan toimituksen yleisten hyvien käytäntöjen mukaisesti.

2.3 Riittämätön tietosuoja

Tietosuojaa koskee seuraava vaatimus. Osoita vaatimuksen toteutuminen käyttäen tarkastuslistaa.

	Vaatimustenmukainen	Ei sovellu	Ei tietoa	Vaatimus ei täyty
Valmistajan tulee tarjota kuluttajille palveluista ja tuotteista selkeää ja läpinäkyvää tietoa siitä, mitä henkilötietoa käsitellään, miten sitä käytetään, kuka sitä käyttää ja mihin tarkoitukseen. Tämä koskee myös Tuotteeseen liittyviä kolmansia osapuolia, kuten mainostajia (ETSI 6.1).	☒	☐	☐	☐

Kuvaa kuinka varmistetaan, että Tuotteen tai Palvelun sisältämää yksilöivää henkilötietoa käsitellään ja varastoidaan käyttäjälle läpinäkyvällä tavalla ja siten, että se rajoittuu vain toiminnallisuuden kannalta välttämättömään.

Palvelu käsittelee yksilöiviä henkilötietoja hyvin rajoitetusti ja vain välttämättömiltä osin – esimerkiksi nimitietoja ei kerätä lainkaan. Palvelun tietosuojaseloste on esillä sekä Wattisen verkkosivuilla että loppukäyttäjäsovelluksessa sisältäen erillisen tiivistelmäversion nopeaa ja helppoa tarkastelua varten.

Voit käyttää seuraavaa taulukkoa yksilöivän henkilötiedon kuvaamiseen. Tietojen luetteloinnin auttaa niiden arvioinnissa.

Yksilöivä henkilötieto	Tuote/Palvelu/Komponentti	Tarkoitus	Henkilötiedon käsittelijä
Käyttäjän puhelinnumero	Palvelu	Käyttäjän tunnistus mobiilisovelluksessa.	DNA Oyj
Käyttäjän älypuhelimen käyttöjärjestelmä ja versio	Palvelu	Ongelmatilanteiden tunnistaminen.	DNA Oyj

Yksilöivä henkilötieto	Tuote/Palvelu/Komponentti	Tarkoitus	Henkilötiedon käsittelijä
Käyttäjän asunnon osoite	Palvelu	Käyttäjän ja termostaattien linkittäminen.	DNA Oyj
Asunnon huoneiden määrä ja tyyppi	Palvelu	Käyttäjän ja termostaattien linkittäminen. Parannettu käyttökokemus.	DNA Oyj
Linkitetyt termostaatit (Tuotteet)	Palvelu	Käyttäjän ja termostaattien linkittäminen.	DNA Oyj
Termostaatin lämpötila	Tuote, Palvelu	Lämpötilan älykäs ohjaus.	DNA Oyj

2.4 Turvaton tiedon siirto ja varastointi

Tiedon siirtoa ja säilytystä koskevat seuraavat vaatimukset. Osoita kunkin vaatimuksen toteutuminen käyttäen tarkastuslistaa.

	Vaatimustenmukainen	Ei sovellu	Ei tietoa	Vaatimus ei täyty
	☐	☒	☐	☐
Tietoturvamielessä arkaluontoiset parametrit tulee pysyvässä säilytyksessä tallentaa laitteeseen turvallisesti (ETSI 5.4-1).				
IoT-kuluttajalaitteessa tulee käyttää kryptografian parhaita käytäntöjä turvallisen viestinnän varmistamiseksi (ETSI 5.5-1).	☒	☐	☐	☐
Valmistajan tulee noudattaa tietoturvallisia hallintaprosesseja laitteen kriittisten tietoturvaparametrien käsittelyssä (ETSI 5.5-8).	☒	☐	☐	☐

Kuvaa, miten Tuote ja/tai Palvelu sekä niiden välinen viestintä on suojattu salauksen ja pääsynhallinnan puutteita vastaan. Salasanojen suojaamisessa tässä käytetään tyypillisesti tiivistysfunktioita.

Palvelussa loppukäyttäjän mobiilisovelluksen ja DNA Oyj:n taustajärjestelmän välillä käytetään TLS/HTTPS-salausprotokollaa. Vastaavasti taustajärjestelmän eri osat kommunikoivat samaa TLS/HTTPS-salausprotokollaa käyttäen. Kaikki kommunikaatio Tuotteisiin tapahtuu DNA Oyj:n yksityisessä APN-verkossa. TLS/HTTPS-sertifikaattien salausavaimet hallitaan Amazon Web Servicesin Certificate Managerissa automaattisesti. Palvelun päivitykseen liittyviä avaimia hallitaan salasananhallintatyökalussa. DNA Oyj:n edustajat pääsevät kirjautumaan Palvelun järjestelmiin vain DNA:n omasta sisäverkosta käsin henkilökohtaisilla tunnuksilla. Ylläpidon salasanojen tiivisteet on muodostettu pbkdf2_sha256-mekanismilla (150000 iteraatiota) ja tallennettu tietokantaan.

2.5 Turvattomat verkkopalvelut ja ekosysteemirajapinnat

Verkkopalveluita ja ekosysteemirajapintoja koskevat seuraavat vaatimukset. Osoita kunkin vaatimuksen toteutuminen käyttäen tarkastuslistaa.

	Vaatimustenmukainen	Ei sovellu	Ei tietoa	Vaatimus ei täyty
Verkon kautta tehtävät, tietoturvan kannalta merkittävät muutokset vaativat tunnistautumista (ETSI 5.5-5).	☒	☐	☐	☐
Kaikki toiminnallisuuksien kannalta tarpeettomat verkon ja loogiset rajapinnat tulee poistaa käytöstä (ETSI 5.6-1).	☒	☐	☐	☐
Ohjelmiston tulisi toimia mahdollisimman vähillä käyttöoikeuksilla huomioiden sekä tietoturvan että toiminnallisuudet (ETSI 5.6-7).	☒	☐	☐	☐

IoT-kuluttajalaitteen tulee tarkastaa kaikki eri rajapintojen kautta tulevat syötteet. Erityisesti käyttöliittymän ja verkkorajapintojen kautta tulevat (ETSI 5.13-1).	☒	☐	☐	☐

Kuvaa miten Tuote on suojattu haavoittuvuuksilta avoimissa verkkopalveluissa, kuten verkkorajapinnoissa ja etähallinnassa. Ota huomioon myös radiorajapinnat.

Kuvaa miten Tuotteen avoimet verkkorajapinnat on suojattu esimerkiksi luvattomalta tunkeutumiselta tai tietovuodoilta.

Nämä rajapinnat liittyvät tyypillisesti pilvipalveluihin ja etähallintaan.

Tuotteet ovat DNA Oyj:n ja asunto-osakeyhtiön sopimuksen keston ajan yhteydessä vain DNA Oyj:n ylläpitämän yksityisen APN-verkon kautta Palvelun komponentteihin.

Palvelussa näkyy verkkoon kaksi porttia. Autentikointiin liittyvä Amazon Web Services Cognito -palvelun autentikointirajapinta tarjoaa mobiilisovellukselle käyttökelpoisia tokeneita pyynnöstä. Mobiilisovelluksen käyttämä HTTPS-portti vaatii Cognitolta saadun tokenin kaikissa pyynnöissä.

Seuraavaa taulukkoa voidaan käyttää vastattaessa kohtiin 2.4 ja 2.5. Tuotteen ja/tai Palvelun testaamisessa käytettävien työkalujen ja menetelmien listaaminen auttaa niiden arvioimisessa.

Verkkoportti / Radioteknologia	Salaus / Pääsynhallinta	Käyttö

2.6 Turvattomat oletusasetukset

Turvattomia oletusasetuksia koskee seuraava vaatimus. Osoita kunkin vaatimuksen toteutuminen käyttäen tarkastuslistaa.

	Vaatimustenmukainen	Ei sovellu	Ei tietoa	Vaatimus ei täyty
IoT-kuluttajalaitteen kuluttajalta vaatimat päätökset käyttöönotossa ja ylläpidossa tulee minimoida. Lisäksi tulee noudattaa tietoturvallisuuden käytettävyyden parhaita käytäntöjä (ETSI 5.12-1).	☒	☐	☐	☐

Kuvaa miten Tuote ja/tai Palvelu on suojattu turvattomilta tehdas- tai oletusasetuksilta. Kuvaa myös, miten käyttäjää opastetaan ylläpitämään turvallisia asetuksia.

Tuote ja Palvelu otetaan asunto-osakeyhtiökohtaisesti käyttöön DNA Oyj:n asiantuntijoiden toimesta. DNA Oyj huolehtii sopimuksen voimassaolon mukaisesti Tuotteen ja Palvelun tietoturvasta. Loppukäyttäjällä ei ole mahdollisuutta esimerkiksi ottaa turvattomia tehdas- tai oletusasetuksia käyttöön.