TUNNISTUSPERIAATTEET

hightrust.id
MEGICAL OY

Vahvan sähköisen tunnistamisen palvelut tarjoaa **Megical Oy (Megical)**, Lapinlahdenkatu 16, 00180 Helsinki, Y-tunnus 2401362-3. Näitä tunnistusperiaatteita sovelletaan Megicalin Suomessa tarjoamiin vahvan sähköisen tunnistamisen palveluihin. Tuote on tunnistuspalvelu, jonka tuotenimi on hightrust.id.

1. PALVELUKUVAUS JA TOIMINTAPERIAATE

hightrust.id on Megicalin kehittämä ja toimittama tunnistuspalvelu, joka tarjoaa loppukäyttäjän tunnistamisen palvelut sitä käyttäville asiointipalveluille. Palvelun käyttö perustuu joko Megicalin omaan tai Suomen valtion julkaisemiin tunnistusvälineisiin. Megicalin oma tunnistusväline tarkoittaa loppukäyttäjän puhelimeen ladattua wallettia. Suomen valtion julkaisemalla tunnistusvälineellä tarkoitetaan valtion julkaisemaa etäluettavaa NFC-korttia.

Megicalin oma tunnistusväline on tuotenimeltään hightrust.id Wallet. Tätä käytettäessä ohjelmisto tarjoaa fyysisen henkilökortin tietojen sekä varmenneketjun liittämisen mobiililaitteeseen hightrust.id-lompakkoon, jolloin fyysistä sirukorttia ei tarvita enää ensitunnistamisen jälkeen. Henkilökortin voi provisioida uuteen mobiililaitteeseen suorittamalla ensitunnistamisen fyysisen henkilökortin avulla.

Palvelua käytettäessä hightrust.id suorittaa käyttäjän autentikoinnin, josta asiointipalvelu saa käyttöönsä autentikoinnin tuloksen sekä loppukäyttäjän tiedot.

1.1. TUNNISTUSPALVELU

Järjestelmä sisältää natiivin mobiilisovelluksen (Mobiilisovellus) sekä pilvipalveluna tarjottavan tunnistuspalvelun (Palvelinjärjestelmä) mobiili-, työpöytä-, sekä web -pohjaisille asiakassovelluksille. Mobiilisovellus tarjoaa tietoturvallisen tunnistustoiminnallisuuden sekä suojatun kommunikaation henkilökortin ja Palvelinjärjestelmän kanssa, kuljettaen sinne kortilta luettua tietoa. Palvelinjärjestelmä puolestaan tarkistaa sovellukselta saadun tiedon avulla tapahtuman oikeellisuuden, varmentaa varmenneketjun DVV-integraation kautta, sekä palauttaa tunnistus tapahtumaa pyytäneelle asiakassovellukselle tuloksen sekä käyttäjän julkisen varmenteen sisältäen käyttäjän tiedot.

hightrust.id tarjoaa SDK:t asiakasorganisaation käyttöön sovelluksien integroimiseksi palveluun. SDK:n avulla integraatio toteutetaan vallitsevaa auktorisointiprotokollaa(oAuth2) sekä sen päälle toteutettua tunnistuskerrosta(Open ID Connect) käyttäen.

Integraation tuloksena asiakassovelluksiin voidaan kirjautua vahvasti hightrust.id Wallet -sovelluksella tai suoraan etäluettavalla henkilökortilla.

1.2. TUNNISTUSVÄLINE

hightrust.id hyödyntää kahta erityyppistä tunnistusvälinettä. Toimiessaan puhelimella käytettävänä kortinlukijana palvelu tukee asiakirjoja, jotka on esitetty tämän dokumentin osiossa ”Ensitunnistaminen”.

hightrust.id voi myös toimia itsessään tunnistuvälineenä. Tällöin tuotenimi on hightrust.id Wallet(”Wallet”). Wallet on puhelimessa toimiva mobiililompakko, johon ensitunnistautuminen suoritetaan valtion julkaisemilla korteilla, jotka on esitetty tämän dokumentin osiossa ”Ensitunnistaminen”.

DVV on julkaissut henkilökorttiin liittyvät käyttöehdot, vastuut ja tunnistusperiaatteet osoitteessa: https://dvv.fi/kansalaisvarmenne-ja-sahkoinen-henkilollisyys

1.2.1. ENSITUNNISTAMINEN

Luottamusverkostossa hightrust.id Walletia käyttöön otettaessa loppukäyttäjän ensitunnistaminen tunnistusvälineen myöntämistä varten tapahtuu toisen tunnistusvälineen liikkeellelaskijan vahvaa sähköistä tunnistetta käyttämällä ja varmentamalla uuden tunnistusvälineen käyttöönotto allekirjoittamalla hyväksytyn välineen allekirjoitusavaimia käyttäen. Hyväksyttyjä välineitä ensitunnistuksessa ovat:

- Suomen valtion myöntämä henkilökortti (11.1.2021 alkaen myönnetyt)
- Organisaatiokortti (19.12.2019 alkaen myönnetyt)

Luottamusverkoston ulkopuolella hightrust.id tarjoaa ensitunnistamisen myös DVV:n myöntämällä sosiaali- ja terveydenhuollon ammattikortilla (myöntämisvuosi 2021 tai uudempi).

Vahvan sähköisen tunnistusvälineen myöntäminen edellyttää, että henkilöllä on Suomen väestörekisteriin merkitty henkilötunnus.

2. PALVELUN KÄYTTÖ JA HINNOITTELU

Palvelun käyttäjiä ovat Megicalin tarjoamiin tunnistuspalveluihin kytkeytyneet asiointipalvelut. Tunnistuspalvelun käyttöön sovelletaan kulloinkin voimassa olevia käytettävien palvelujen yleisiä

ehtoja sekä asiointipalveluiden kanssa mahdollisesti erikseen sovittavia tapauskohtaisia ehtoja. Palveluntarjoajan ja asiointipalvelun välillä noudatetaan sovittuja hintoja.

Mobiilisovellus ladataan iPhone-puhelimiin Applen App Storesta ja Android-puhelimiin Google Playsta. Loppukäyttäjä hyväksyy sovelluksiin liittyvät yleiset ehdot sovelluksen lataamisen yhteydessä.

3. TUNNISTUSPALVELUN VARMUUSTASO JA TURVALLISUUSJOHTAMINEN

Megicalilla on tunnistuspalvelun toteuttamiseksi tunnistuslakiin perustuva oikeus käsitellä loppukäyttäjän henkilötietoja. Megicalin tuottaman tunnistuspalvelun varmuustaso on korotettu. Megicalin turvallisuustoiminnan päämääränä on Megicalin maineen ylläpitäminen luotettavana yhteistyökumppanina, liiketoiminnan ja palveluiden jatkuvuuden turvaaminen, Megicalin käytössä olevien tietojen ja omaisuuden suojaaminen, henkilöstön työkyvyn, turvallisuuden ja turvallisuustietoisuuden ylläpito sekä asiakkaiden luottamuksen säilyttäminen.

4. TARJOTTAVAT PALVELUT JA NIIHIN SOVELLETTAVAT EHDOT

Megical tarjoaa tunnistusvälinettä sekä tunnistusvälityspalvelua ja on rekisteröity palveluntarjoajana Liikenne- ja viestintäviraston tunnistuspalvelurekisteriin. Palvelujen vaatimustenmukaisuus varmistetaan kohdistamalla palveluihin säännöllisiä arviointeja. Megicalin tunnistusväline on tietoturvaltaan ja tasoltaan eIDAS asetuksessa (EU 910/2014) määritellyn tason ”korotettu” mukainen.

5. TUNNISTUSVÄLINEEN KÄYTTÖRAJOITUKSET

Tunnistusvälineellä tehtyjä tunnistustapahtumia ei saa välittää lain taikka hyvän tavan vastaisiin tarkoituksiin. Megicalin tunnistusvälineen haltijalle ei saa luoda uutta Tunnistuslain mukaista vahvaa sähköistä tunnistusvälinettä, ellei tunnisteen luomisesta ole sovittu Megicalin kanssa ja ellei Megicalille välitetä tietoa ketjutuksesta. Ketjutettua tunnistetta, joka ei ole Tunnistuslain mukainen vahva sähköinen tunnistusväline, saa käyttää tai hyödyntää vain tunnisteen luoneen asiointipalvelun palveluntarjoajan omissa palveluissa.

6. TIETOSUOJAPERIAATTEET JA TUNNISTUSMENETELMÄN TIETOTURVALLISUUS

Megical noudattaa tunnistuspalveluja tarjotessaan henkilötietojen käsittelyä koskevaa lainsäädäntöä. Henkilötietojen käsittelystä kerrotaan Megicalin tietosuojaselosteessa. Megicalilla on oikeus välittää tunnistustiedot asiointipalvelun tarjoajalle tai asiointipalvelun käyttämälle tunnistusvälityspalvelulle tilanteissa, joissa loppukäyttäjä tunnistautuu näiden palveluihin.

Tunnistautuva loppukäyttäjä lukee Megicalin tunnistautumispalvelua käyttäessään oman tunnistusvälineensä(sirukortit tai higtrust.id Wallet) ja vahvistaa tunnistautumisen antamalla sovellukseen PIN-koodinsa. Loppukäyttäjä voi halutessaan korvata PIN-koodin mobiililaitteensa hallinnoimalla biometrisella tunnisteella(sormenjälki tai kasvokuva).

Kaikesta tunnistukseen liittyvästä toiminnasta pidetään lokia, jota säilytetään vähintään viisi (5) vuotta.

Megicalin ohjelmisto tallentaa tapahtumat ja virhetilanteet AWS:n lokijärjestelmään. Myös mittaroidut järjestelmätapahtumat ja vikatilanteet tallennetaan. Tekniset ongelmat sekä poikkeamat tulevat vastaavan tiimin tietoon automaattisten hälytysten kautta suojatuille kanaville riippuen hälytyksen tyypistä.

Järjestelmästä tuotetaan lisäksi erillistä audit-lokia, johon jokainen yksittäinen tunnistustapahtuma tallennetaan. Tämän perusteella kaikki tiettyyn tunnistustapahtumaan liittyvät tiedot ovat todennettavissa. Audit-lokin käytöstä tallennetaan vielä erillinen loki, josta mahdollinen audit-lokin käsittely ilmenee. Audit-loki ja sen “lokin loki” on tallennettu AWS:ään Tukholmaan erillisille virtuaalipalvelimille.

Kukin tunnistustapahtuman osapuoli vastaa omien palveluittensa suojauksesta, turvallisuudesta ja säilyttämiensä tietojen oikeellisuudesta. Tunnistautuva loppukäyttäjä vastaa siitä, että Megicalin antamat tunnistautumisvälineet eivät joudu ulkopuolisten haltuun.

7. VALVONTAVIRANOMAISET

Liikenne- ja viestintävirasto Traficom valvoo vahvan sähköisen tunnistamisen palveluita.

PL 320, 00059 TRAFICOM
puh. 02 9534 5000
www.traficom.fi

Megical Oy:n toimintaa valvovat myös valtuuksiensa puitteissa Suomen kuluttaja-asiamies ja muut suomalaiset viranomaiset.