

Terveysthuollon puhelinalveluun soittavan henkilön tunnistaminen asioitaessa tekoälyavustajan kanssa

Taustaa

Terveysthuollossa valtaosa yhteydenotoista on perinteisesti tehty soittamalla puhelinalveluun. Digitaalisten asiointipalveluiden yleistyttyä puhelumäärät ovat hieman laskeneet, mutta ne ovat edelleen merkittäviä. Uudet kielimallipohjaiset tekoälyavustajat mahdollistavat digipalveluita vastaavat itsepalvelut puhelinalveluissa. Terveysthuollossa huomataan viimeistään uusien palveluiden arviointi- ja käyttöönottovaiheissa [asiakastietolain 8 §:n](#) vaatimus asiakastietojen käsittelyyn osallistuvien luotettavasta tunnistamisesta.

Käsitlemme tässä oppaassa erilaisten puhelinalveluun soveltuvien tunnistamistapojen vahvuuksia ja heikkouksia käytettävyyden, tietoturvan ja regulaation näkökulmasta. Keskitymme tässä oppaassa asiakastietolain vaatimukseen, vaikka tunnistamistarve voi liittyä laajempaan lainsäädäntökehikseen.

Puhelinalveluissa tehdään toistaiseksi enemmän yhteydenottoja kuin digipalveluissa. [Digipalvelulaki ei koske puhelinalveluita](#), joten digipalveluiden käyttämien automaatioiden ja rajapintojen hyödyntäminen puhelinalvelussa tekoälyavustajan kanssa on houkutteleva vaihtoehto. Lähitulevaisuudessa todennäköisesti selviää ovatko puhelinalveluiden tekoälyavustajia koskevat vaatimukset kuitenkaan digipalveluiden vaatimuksia kevyempiä, kun kyseessä on käytännössä samojen taustajärjestelmien avulla tuotettu sähköinen itsepalvelu.

Tavallisimmat tunnistamiskeinot puhelinalvelussa

Puhelinalveluun soittavan henkilön tavallisimpia tunnistamiskeinoja ovat:

1. Turvakysymykset.
2. Ennalta jaettu salaisuus (koodi).
3. Puhelinverkon ilmoittama puhelinnumero.
4. Soittajan ääni.
5. Vahva sähköinen tunnistaminen.
6. Muun tunnistusratkaisun (älypuhelinsovellus) hyödyntäminen.

Turvakysymykset

Henkilöltä kysytään yhtä tai useampaa riittävän salaista tietoa hänen tunnistamiseksi. Tietojen pitää olla henkilön itsensä ja tunnistavan organisaation tiedossa.

Edut:

- + Soveltuu natiivisti puhelun aikana kysyttäväksi.
- + läkkäälle väestölle usein helpoin vaihtoehto.

Haasteet:

- Hyvän yhteisen salaisuuden löytäminen on usein haastavaa tai mahdotonta.
- Saako salaisuutta, esimerkiksi potilastietoa, käsitellä tunnistamistarkoituksessa, kun kaikkia käsittelyyn osallistuvia ei vielä ole tunnistettu?
- Ei mahdollista toisen henkilön puolesta asiointia.

Henkilötunnuksesta turvakysymyksenä

Perinteisesti Suomessa on totuttu kysymään henkilötunnusta, vaikka sitä ei ole alunperin tarkoitettu henkilön tunnistamiseen vaan henkilön yksilöimiseen. Yksilöimistarkoitus edellyttää, että henkilötunnus on pysyvä. Henkilötunnusta myös käsitellään hyvin monessa eri asiointiyhteydessä, joten henkilötunnus ei pysy salaisena. Pelkän henkilötunnuksen tai henkilötunnuksen ja nimen yhdistelmän kysyminen tunnistamistarkoituksessa on kielletty [tietosuojalain 29.5 §](#):ssä 1.1.2024 alkaen, koska henkilötunnusta on yksilöimistarkoituksen lisäksi käytetty tunnistamiseen, jonka johdosta henkilötunnusten avulla on tehty paljon identiteettivarkauksia. [HE 62/2023](#) mukaan puhelinasioinnissa tapahtuva tunnistaminen tulisi rakentaa siten, että tunnistettavalta henkilöltä kysyttäisiin henkilötunnuksen lisäksi muitakin tunnistetietoja, kuten asiakasnumeroa tai muita asiakassuhteelle tyypillisiä lisätietoja, jotka eivät olisi helposti kaikkien saatavilla. Esimerkiksi kotikunta- tai osoitetietoa ei voitaisi pitää riittävinä lisätietoina henkilön varman ja luotettavan tunnistamisen kannalta.

Ennalta jaettu salaisuus

Ennalta jaettu salaisuus voi olla esimerkiksi ajanvaraustunnus tai ajanvarusluvan yhteydessä toimitettu salaisuus (koodi). Tekoälyavustaja voi helposti kysyä tätä salaisuutta tai sen voi syöttää ennalta puhelinpalvelun IVR-valikossa. Koodin voi toimittaa esimerkiksi kirjeellä tai tekstiviestillä, jolloin se on kirje- ja viestintäsalaisuuden suojaama. Koodi voi myös olla kertakäyttöinen tai rajattu ajallisesti. Vaarantuneen koodin voi myös vaihtaa tai mitätöidä tarvittaessa, vaikka se olisi pidempään voimassa.

Edut:

- + Soveltuu natiivisti puhelun aikana kysyttäväksi.
- + Ei liity laadukkaan turvakysymyksen määrittämiseen liittyvää haastetta.

Haasteet:

- Salaisuuden toimitustavan hinta.
- Salaisuuden toimitustavan hitaus.
- Pitää olla toimitettuna ennen asiointia.
- Ei mahdollista toisen henkilön puolesta asiointia.
- Käytettävyys varauksin.

Puhelinverkon ilmoittama puhelinnumero

Puhelinpalveluun soittavalla henkilöllä on yleensä numeronnäyttö päällä. Puhelinverkon ilmoittaman puhelinnumeron voi yhdistää taustarekisterissä olevaan henkilön ilmoittamaan puhelinnumeroon. Tietoturvan näkökulmasta puhelinverkon ilmoittama puhelinnumero ei ole kovinkaan luotettava, koska puhelinverkko mahdollistaa ilmoitettavan puhelinnumeron määrittämisen. Tämä on puhelinverkon ominaisuus, mutta valitettavasti se johtaa siihen, [ettei verkon ilmoittamaan puhelinnumeroon voi luottaa](#) (spoofaus).

Edut:

- + Soveltuu natiivisti puhelun aikana kerättäväksi.
- + Ei vaadi interaktiota.

Haasteet:

- Puhelinnumero voi olla salainen.
- Kyseessä ei ole tietoturallinen tapa tunnistaa soittajaa.
- Taustarekisterissä sama puhelinnumero voi olla useammalla ihmisellä, esimerkiksi henkilöllä itsellään ja tämän lapsella.

Soittajan ääni

Puhelinpalveluissa on maailmanlaajuisesti käytetty myös puhelinpalveluun soittavan henkilön ääntä tämän tunnistamiseksi. EU-alueella tietosuoja-asetus (GDPR) asettaa kuitenkin tiettyjä rajoitteita biometrisen tiedon käsittelylle. [Tietosuojavaltuutetun toimiston mukaan](#) henkilöllisyyden vahvistamisessa on noudatettava tietojen minimoinnin periaatetta, eikä henkilöllisyyden vahvistamista varten lähtökohtaisesti saa kerätä enempää tietoja kuin rekisterinpitäjällä on jo hallussaan. Tästä johtuen äänitiedon kerääminen pelkkää tunnistautumistarkoitusta varten voi olla laillisuusnäkökulmasta haastavaa. Tietoturvaan liittyvä uusi ongelma on se, että isot kielimallit ovat erittäin kyvykkäitä avustamaan ns. deepfake hyökkäyksissä ja äänen kloonaaminen onkin nykyään triviaalia.

Edut:

- + Soveltuu natiivisti puhelun aikana kerättäväksi.
- + Ei vaadi interaktiota.

Haasteet:

- Saako biometrisen äänitiedon kerätä tunnistamistarkoitusta varten.
- Biometrisen äänitiedon pitää olla kerättynä etukäteen.
- Ei kovin tietoturvallinen tunnistamistapa deepfakejen yleistyttyä.

Vahva sähköinen tunnistaminen

[Vahva sähköinen tunnistaminen](#) on etänä tapahtuvan henkilöllisyyden varmentamisen kultainen standardi Suomessa. Toisen puolesta asiointi Suomi.fi-valtuuksien avulla edellyttää vahvan sähköisen tunnistamisen käyttöä. Osalle ihmisistä vahvan sähköisen tunnistamisen ja digipalveluiden käyttö [on kuitenkin haastavaa](#). Mikään tunnistautumismenetelmä ei kuitenkaan takaa 100 % onnistumista. Carecode Oylla on usean vuoden kokemus puhelinpalveluiden vahvasta sähköisestä tunnistamisesta ja tyypillinen onnistumis-% vaihtelee sektorista ja demografiasta riippuen 60–85 % välillä. Suosittelemme mallia, jossa kaikki tunnistautumiskykyiset pyritään tunnistamaan vahvasti ja tarjotaan muille asiakasryhmille nopea pääsy asioimaan ihmisen kanssa.

Vahvaa sähköistä tunnistautumista voi käyttää puhelinpalvelun kanssa muutamalla eri tavalla. Tyypillisin on puhelun aikana tekstiviestitse toimitettava linkki, jonka kautta pääsee tunnistautumaan. On myös ratkaisuja, joissa tunnistautuminen tehdään ennen puhelinpalveluun soittamista. Näissä haasteena on se, että puhelinpalveluun soittavan pitää tietää tunnistautumisen tarve etukäteen, eikä tunnistautumista voi tehdä tarvittaessa puhelun aikana. Esimerkiksi [Verohallinto](#) ja [Kela](#) tarjoavat tällaisen etukäteisen tunnistautumisen mahdollisuutta.

Tekstiviesti on nykyään luotettava, nopea ja varmatoiminen tapa lähettää tunnistautumispyyntö puhelinpalveluun soittavalle henkilölle. Traficom [määräys](#) vaatii teleoperaattoreita estämään toisen organisaation nimissä (lähettäjä tunnukseksi) lähetettävät tekstiviestit SMS rajapinnoissaan ja tämä vaatimus estää perinteisiä tietojenkalasteluviestejä tehokkaasti.

Edut:

- + Luotettavin tapa tunnistaa puhelinpalveluun soittava henkilö.
- + Mahdollistaa regulaation puolesta kaikki eri käyttöskenaariot.
- + Kansalaisille tuttu ja laajasti käytössä oleva tunnistautumistapa.
- + Mahdollistaa puolesta asiointin Suomi.fi-valtuuksien avulla.
- + Täyttää automatisoidun HTAn tunnistamisvaatimuksen ([HE 199/2026](#)).

Haasteet:

- Käytettävyys varauksin.
- Hinta verrattuna rajakustannuksettomiin vaihtoehtoihin.

Muun tunnistusratkaisun (älypuhelinsovellus) hyödyntäminen

Vahvalle sähköiselle tunnistamiselle on myös kilpailevia sähköisiä tunnistautumISRatkaisuja. Näitä on esimerkiksi organisaation oma älypuhelinsovellus ja [MobilePay](#). Näissä henkilön pitää tyypillisesti asentaa etukäteen sovellus ja tunnistautua sovellukseen sen käyttöönoton yhteydessä. Organisaation omaan sovellukseen pohjautuva tunnistautuminen ei toimi puhelun aikana, jos puhelinpalveluun soittava henkilö ei ole asentanut tunnistautumiseen käytettävää sovellusta etukäteen. [Julkisella sektorilla on tukipalvelulain nojalla velvollisuus käyttää Suomi.fi-tunnistusta](#), mikä vähentää oman tunnistautumissovelluksen mielekkyyttä julkisella sektorilla.

Edut:

- + Omassa sovelluksessa on organisaation oma brändi.
- + Parhaimmillaan käytöstä ei aiheudu rajakustannuksia.
- + Tunnistautumispyyntö voidaan lähettää suoraan tunnistussovellukseen.

Haasteet:

- Ei ole tunnistamislaisissa tarkoitettua vahvaa sähköistä tunnistamista.
- Ei mahdollista Suomi.fi-valtuuksien hyödyntämistä.
- Sovelluksen pitää olla asennettuna tunnistautumishetkellä.
- Luvitukseen liittyy ajoittain teknisiä ongelmia (permissions), jos sovellusta käytetään harvakseltaan.

Lopuksi

Yllä esitetyt vaihtoehdot havainnollistavat sen, että puhelinpalveluun soittavan henkilön tunnistamisen voi tehdä monella tapaa. Käytännössä näin onkin pakko tehdä, koska yhdellä tavalla ei koskaan pysty mahdollistamaan asiointia kaikille. Carecode Oyn [Tunnistaja](#) mahdollistaa puhelinpalveluun soittavan henkilön vahvan sähköisen tunnistamisen Suomi.fi-tunnistuksen tai yksityisen tunnistuspalvelun avulla. Tunnistajaa voi tämän lisäksi käyttää myös organisaation omaa autentikaattorin tai MobilePayn kanssa. Viimeisenä tunnistautumiskeinona puhelinpalveluun soittavalle kannattaa pääsääntöisesti tarjota turvakysymyksiä. Soittaja voidaan aina ohjata keskustelemaan ihmisen kanssa, jos turvakysymyksiä ei voi syystä tai toisesta hyödyntää tekoälyavustajan kanssa.