

A woman with long blonde hair and a young girl with blonde hair are smiling and pointing towards the right. The woman is wearing a purple patterned top, and the girl is wearing a white shirt and blue overalls. They are outdoors on a wooden deck with a white building and greenery in the background.

Mobiilivarmenne

Heidi Havastila, DNA Oyj

Sisältö

Mikä on Mobiilivarmenne?

Mitä tarkoitetaan vahvalla sähköisellä tunnistautumisella ja mihin sitä tarvitaan?

Miksi Mobiilivarmenne kannattaa ottaa käyttöön?

Miksi Mobiilivarmenne voi olla pankkitunnuksia turvallisempi tapa tunnistautua ja miksi tunnistustapoja kannattaa olla useampi?

Miten Mobiilivarmenne otetaan käyttöön ja miten sitä käytetään?

Miten Mobiilivarmenne otetaan käyttöön omalta operaattorilta ja miten sitä käytetään palveluissa tunnistautumiseen?



Mikä on Mobiilivarmenne?

Mitä tarkoitetaan vahvalla sähköisellä tunnistautumisella ja mihin sitä tarvitaan?

Mitä tarkoitetaan vahvalla sähköisellä tunnistautumisella?

- Vahvalla sähköisellä tunnistautumisella tarkoitetaan **henkilöllisyyden todentamista** sähköisesti.
- Vahvan tunnistautumisen avulla
 - Kuluttajat voivat turvallisesti vahvistaa henkilöllisyytensä erilaisissa sähköisissä palveluissa
 - Sähköisten **asiointipalveluiden tarjoajat voivat luotettavasti tunnistaa asiakkaansa**
- Liikenne- ja viestintäviraston kyberturvallisuuskeskus valvoo sähköisen tunnistamisen palveluja.
 - Varmistetaan palveluiden luotettavuus, tietoturvallisuus sekä säädettyjen vaatimusten noudattaminen



Mitä ovat vahvat sähköiset tunnistuspalvelut?

- Suomessa vahvoja sähköisiä tunnistuspalveluita ovat
 - Teleoperaattoreiden **Mobiilivarmenteet**
 - Pankkien **verkkopankkitunnukset**
 - Digi- ja väestötietoviraston **kansalaisvarmenne** (poliisin myöntämällä henkilökortilla)

Valitse tunnistustapa



Varmennekortti



Mobiilivarmenne



Osuuspankki

Nordea

Nordea



Danske Bank

Handelsbanken

Handelsbanken

ÅLANDSBANKEN

Ålandsbanken



S-Pankki

Aktia

Aktia

POP Pankki

POP Pankki

Säästöpankki

Säästöpankki

omaop

Oma Säästöpankki

Missä palveluissa vahvaa sähköistä tunnistautumista käytetään?

- Vahvaa sähköistä tunnistautumista käytetään palveluissa, joissa asiakkaan henkilöllisyys tulee todentaa.
- Tällaisia palveluita ovat esimerkiksi terveyspalvelut, Kela, OmaVero, Suomi.fi ja Kanta.
- Sähköistä vahvaa tunnistautumista käyttää arviolta yli 20 000 palvelua.

Kela|Fpa[®]


MEHILÄINEN


Terveystalo

Kanta

oma/vero

Mikä on Mobiilivarmenne?

- Mobiilivarmenne on DNA:n, Elisan ja Telian yhteistyössä kehittämä ja ylläpitämä **luotettava vahvan sähköisen tunnistautumisen palvelu.**
- Mobiilivarmenne kulkee aina mukana **puhelimien SIM-kortilla** ja toimii kaikkialla.
- Mobiilivarmenne on operaattorin **puhelinliittymään tilattava lisäpalvelu**, jonka saat käyttöösi omalta operaattoriltasi.
- Mobiilivarmenneen **käyttö on helppoa, nopeaa ja turvallista.**



Mobiilivarmenne

Miksi Mobiilivarmenne kannattaa ottaa käyttöön?

Miksi Mobiilivarmenne voi olla pankkitunnuksia turvallisempi tapa tunnistautua ja miksi tunnistustapoja kannattaa olla useampi?



Miksi Mobiilivarmenne kannattaa ottaa käyttöön?

1. PIDÄ VERKKOPANKKITUNNUKSET TURVASSA HUIJAREILTA

- Suomalaiset ovat pitkään käyttäneet vahvassa sähköisessä tunnistautumisessa pankkien verkkopankkitunnuksia.
 - Valitettavasti viime vuosina verkkopankkitunnuksia kalastelevat huijaukset ovat lisääntyneet hurjaa vauhtia.
 - Verkkopankkitunnukset kiinnostavat taloudellista hyötyä havittelevia verkkorikollisia, koska niillä pääsee suoraan käsiksi uhrin rahoihin.
 - Mobiilivarmenteella ei pääse kirjautumaan pankkipalveluihin, joten Mobiilivarmenne ei ole ollut verkkorikollisten kiinnostuksen kohteena.
- **Nyrkkisääntö:** Käytä verkkopankkitunnuksia ainoastaan pankin omiin palveluihin kirjautuessa ja Mobiilivarmennetta kaikissa muissa palveluissa.

HUIJAUKSET JA PETOKSET

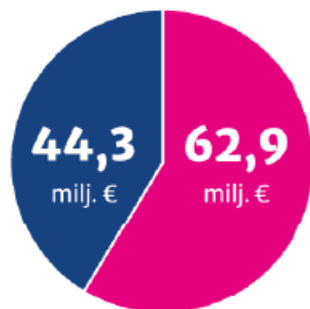
Pankkien tietoon tulleet huijaukset 2024



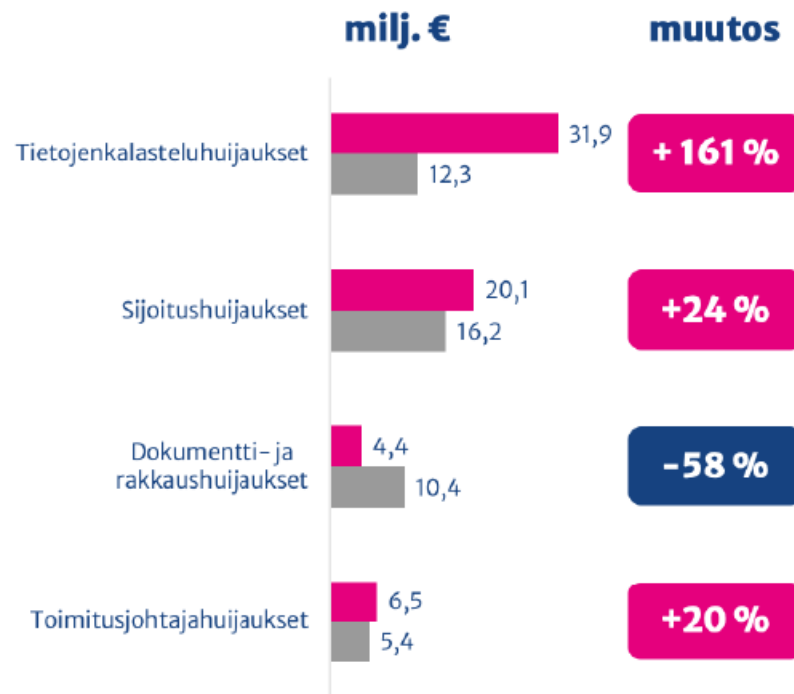
Huijauksia yhteensä 2024

107,2

milj. €

+39 %
vrt. 2023Pankkien
pysäyttämät ja
palauttamatt
maksutSuomalaiset
menettäneet
verkkorikollisille

Lähde: FA





Miksi Mobiilivarmenne kannattaa ottaa käyttöön?

2. VARMISTA PALVELUIDEN SAAVUTETTAVUUS KAHDELLA TUNNISTUSMENETELMÄLLÄ

- Viime aikoina olemme nähneet kasvavan määrän palvelunestohyökkäyksiä, jotka ovat kohdistuneet pankkeihin.
 - Hyökkäysten aikana pankkipalvelut eivät ole olleet käytössä ja siten myöskään verkkopankkitunnuksilla ei ole pystynyt tunnistautumaan muihin palveluihin.
 - Vahvaa sähköistä tunnistautumista käyttävät palvelut voivat olla asiakkaille kriittisiä esim. terveyspalvelut.
 - Varmista palveluiden saavutettavuus ottamalla käyttöön kaksi sähköisen tunnistautumisen palvelua.
- **Nyrkkisääntö:** Jokaisella tulisi olla kaksi eri tunnistautumispalvelua varmistaakseen palveluihin pääsyn myös käyttökatkosten aikana.



Mobiilivarmenne

Poliisi, Kyberturvallisuuskeskus, pankit sekä tietoturvan asiantuntijat suosittelevat pankkitunnusten käyttöä ainoastaan pankkipalveluihin ja Mobiilivarmenteen käyttöä muissa palveluissa.

- 1. PIDÄ VERKKOPANKKITUNNUKSET TURVASSA HUIJAREILTA**
- 2. VARMISTA PALVELUIDEN SAAVUTETTAVUUS KAHDELLA TUNNISTUSMENETELMÄLLÄ**



Voidaanko Mobiilivarmennetta väärinkäyttää?

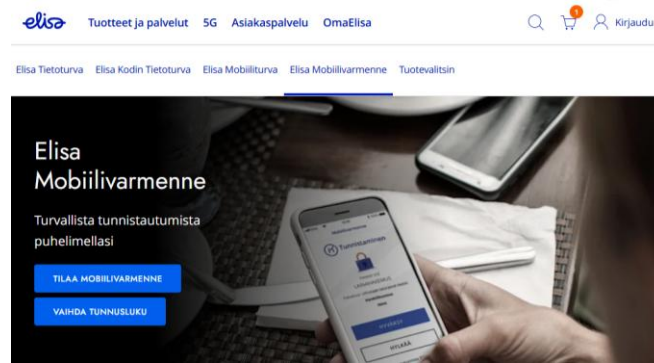
- Verkkorikolliset keksivät uusia tapoja väärinkäytöksille jatkuvasti, mutta **vielä on nähty hyvin vähän huijauksia, joissa kalasteltaisiin Mobiilivarmenteen tietoja.**
- Mobiilivarmenteen väärinkäyttö **vaatisi tunnistustapahtuman hyväksymistä PIN-koodilla** sillä puhelimella, jossa on kyseisen liittymän SIM-kortti.
- Käytännössä **rikollisen pitäisi saada puhelin haltuunsa** sekä ohittaa puhelimen näytön lukitus ja tietää Mobiilivarmenteeseen asetettu PIN-koodi.
- Huijarit voivat myös yrittää tehdä tunnistautumisia palveluihin antamalla uhrin puhelinnumeron ja toivomalla, että sen käyttäjä epähuomiossa hyväksyisi tunnistautumistapahtuman, jota itse ei ole tehnyt.
- Välttääkseen huijausyritykset **Mobiilivarmenteelle kannattaa ottaa käyttöön häirinnänestokoodi**, jolloin puhelinnumeron lisäksi huijarin pitäisi tietää palvelulle asetettu häirinnänestokoodi eli salasana.

Miten otan Mobiilivarmenne otetaan käyttöön?

Miten saat Mobiilivarmenteen käyttöösi omalta operaattoriltasi?

Miten saan Mobiilivarmenneen käyttöön?

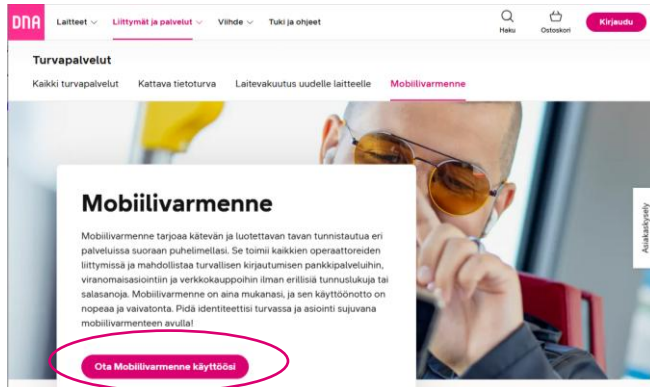
- Mobiilivarmenne on **oman operaattorin** tarjoama puhelinliittymän lisäpalvelu.
- Saadaksesi Mobiilivarmenneen käyttöösi ole siis yhteydessä omaan operaattoriisi:
 - DNA: dna.fi/mobiilivarmenne
 - Elisa: elisa.fi/mobiilivarmenne
 - Telia: telia.fi/mobiilivarmenne
- Mobiilivarmenneen **käyttöönottoon** tarvitset:
 - **Puhelimen, jossa on liittymä**, jolle Mobiilivarmenne otetaan käyttöön
 - **Verkkopankkitunnukset**, joilla todennat henkilöllisyytesi käyttöönotossa
- Mobiilivarmenne **tulee olla sallittuna liittymän** omistajan puolesta liittymälle.



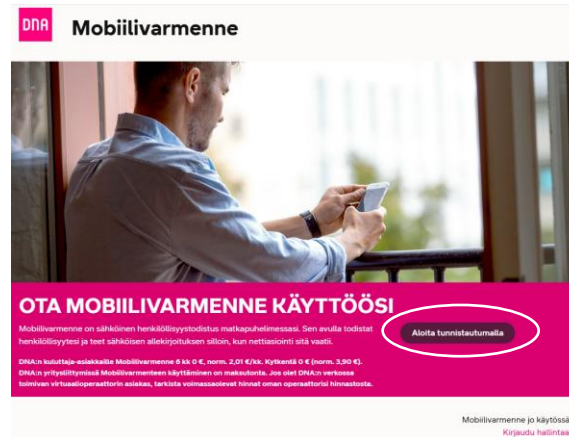
Mobiilivarmenteen käyttöönotto (esimerkkinä DNA:n asiakas)

PALVELUN TIETOJEN ANTAMINEN JA HENKILÖLLISYYDEN TODENTAMINEN

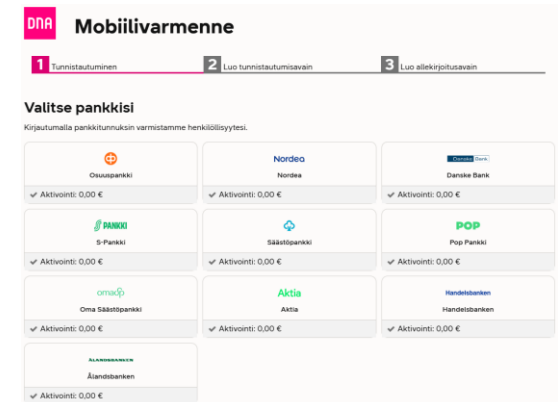
1. Mene osoitteeseen
dna.fi/mobiilivarmenne ja paina ”Ota
Mobiilivarmenne käyttöösi” –painiketta.



2. Saat lisätiedot palvelusta ja sen
hinnoittelusta. Paina ”Aloita
tunnistautumalla” –painiketta.



3. Valitse oma pankkisi ja
tunnistaudu
verkkopankkitunnuksilla.



Mobiilivarmenteen käyttöönotto

LIITTYMÄNUMERON JA SEN HALTIJAN VARMENTAMINEN

4. Syötä liittymäsi puhelinnumero, jolle olet aktivoimassa Mobiilivarmennetta ja paina ”Jatka”.

DNA

Mobiilivarmenne

1

Tunnistautuminen

2

Luo tunnistautumisavain

3

Luo allekirjoitusavain

Syötä seuraavaksi puhelinnumerosi
Mobiilivarmenne liitetään matkapuhelimesi SIM-korttiin.
Anna puhelinnumero, johon haluat liittää mobiilivarmenteen:
Puhelinnumero *

Täytä puhelinnumero muodossa: 0441234567
Jatka

5. Saat liittymääsi tekstiviestitse vahvistuskoodin numerosta 14000. Syötä koodi sille varattuun paikkaan ja paina ”Jatka”

DNA

Mobiilivarmenne

1

Tunnistautuminen

2

Luo tunnistautumisavain

3

Luo allekirjoitusavain

Puhelinnumeron tarkistus
Lähetimme sinulle vahvistusviestin puhelimeesi.
Syötä viestissä lähetetty vahvistuskoodi tähän:
Eikö viesti saapunut?
Tarkista puhelinnumerosi
Vahvistuskoodi *

Jatka

Mobiilivarmenteen käyttöönotto

HENKILÖTIETOJEN VARMISTAMINEN

6. Varmista, että omat tietosi ovat oikein ruksimalla hyväksyntä laatikon ja paina ”Jatka”.

DNA

Mobiilivarmenne

1

Tunnistautuminen

2

Luo tunnistautumisavain

3

Luo allekirjoitusavain

Varmista omat tietosi

Mobiilivarmenne yksilöi henkilöllisyytesi. Tarkastathan, että tietosi ovat oikein.

Eivätkö tiedot täsmää?

Nimi

Henkilötunnus

Puhelinnumero

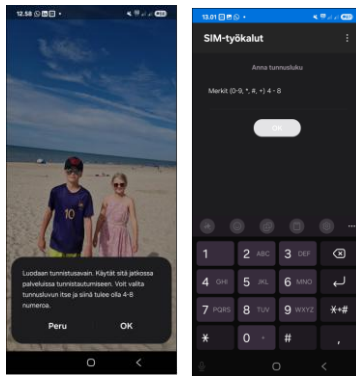
☐ Tiedot ovat oikein ja hyväksyn * käyttöehdot

Jatka

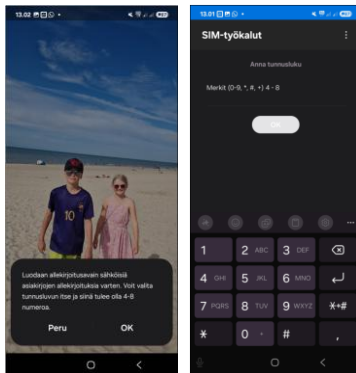
Mobiilivarmenteen käyttöönotto

TUNNISTAUTUMISAVAIMEN (PIN-KOODI) JA ALLEKIRJOITUSAVAIMEN LUONTI

7. Saat puhelimeesi pyynnön luoda tunnistautumisavain, joka toimii Mobiilivarmenteen PIN-koodina hyväksyessäsi tunnistautumistapahtumia.



8. Saat puhelimeesi pyynnön luoda allekirjoitusavain, joka toimii allekirjoittaessasi dokumentteja Mobiilivarmenteella. Allekirjoitusavain voi olla sama kuin tunnistautumisavain.



DNA Mobiilivarmenne

- 1 Tunnistautuminen
- 2 Luo tunnistautumisavain
- 3 Luo allekirjoitusavain

Luo tunnistautumisavain

Tunnistautumisavain on henkilökohtainen koodisi, jolla jatkossa tunnistaudut eri palvelussa.

Voit valita numerosarjan itse. Tunnistautumisavaimessa tulee olla 4-8 numeroa.

Eikö tunnistautumisavaimen luomispyyntö saapunut matkapuhelimeesi?

[Yritä uudelleen](#)



DNA Mobiilivarmenne

- 1 Tunnistautuminen
- 2 Luo tunnistautumisavain
- 3 Luo allekirjoitusavain

Tunnistautumisavain on luotu

Tunnistautumisavaimen lisäksi mobiilivarmenteeseen luodaan allekirjoitusavain, digitaalista allekirjoitusta varten. Voit valita numerosarjan itse. Halutessasi se voi olla sama kuin tunnistautumisavaimessa.

[Jatka](#)



Mobiilivarmenne



VALMISTA TULI!

Mobiilivarmenne on nyt valmiina käyttöösi. Voit kokeilla sitä hallintapaneelissa.

[Kokelle mobiiliva...](#)

Miten otan häirinnänestokoodin käyttööni?

- Häirinnänestokoodi **auttaa huijauksilta suojautumiseen**.
- Kun häirinnänestokoodi on lisätty Mobiilivarmenteelle, tulee tunnistautuessa tietää puhelinnumeron lisäksi myös häirinnänestokoodi eli oma salasanasasi.
- Näin huijari ei voi tehdä tunnistuspyyntöjä pelkällä puhelinnumerolla toivoen, että käyttäjä epähuomiossa hyväksyisi tunnistautumisen.

Häirinnänestokoodi asetetaan Mobiilivarmenteelle seuraavasti:

- **DNA:** Mene DNA:n mobiilivarmenteen hallintapalveluun häirinnänestokoodin asettamiseksi (<https://mobiilivarmenne.dna.fi/mc/login>)
- **Telia:** Lähetä viesti ESTO valitsemasi koodi numeroon 15011. Koodi voi olla enintään 10 merkkiä pitkä, eikä se saa sisältää ääkkösiä.
- **Elisa:** Lähetä viesti STKSPAM koodi numeroon 18258. Koodi voi olla 3–16 merkkiä pitkä numeroista ja kirjaimista koostuva jono, ja sen pitää alkaa kirjaimella.

Ohjeita puhelimen tai liittymän vaihtotilanteeseen?

- **Puhelimen vaihto**

- Mobiilivarmenne on SIM-kortilla oleva palvelu, joten puhelimen vaihto ei vaikuta Mobiilivarmenteen toimintaan. Mobiilivarmenne toimii myös uudella puhelimella, johon siirrät SIM-korttisi.

- **Liittymän vaihto (numeronsiirto)**

- Mikäli vaihdat liittymäsi toiselle operaattorille eli teet numeronsiirron, tulee Mobiilivarmenne ottaa käyttöön uudella operaattorilla. Mobiilivarmenne lakkaa toimimasta vanhalla operaattorilla automaattisesti numeronsiirron astuessa voimaan.

- **Mobiilivarmenteen siirto toiseen liittymään**

- Mikäli otat käyttöösi uuden liittymän, johon haluat siirtää Mobiilivarmenteen, tulee sinun ottaa Mobiilivarmenne uudelleen käyttöön uudella liittymällä ja lopettaa Mobiilivarmenteen käyttö vanhalla liittymällä olemalla yhteydessä operaattorin asiakaspalveluun.

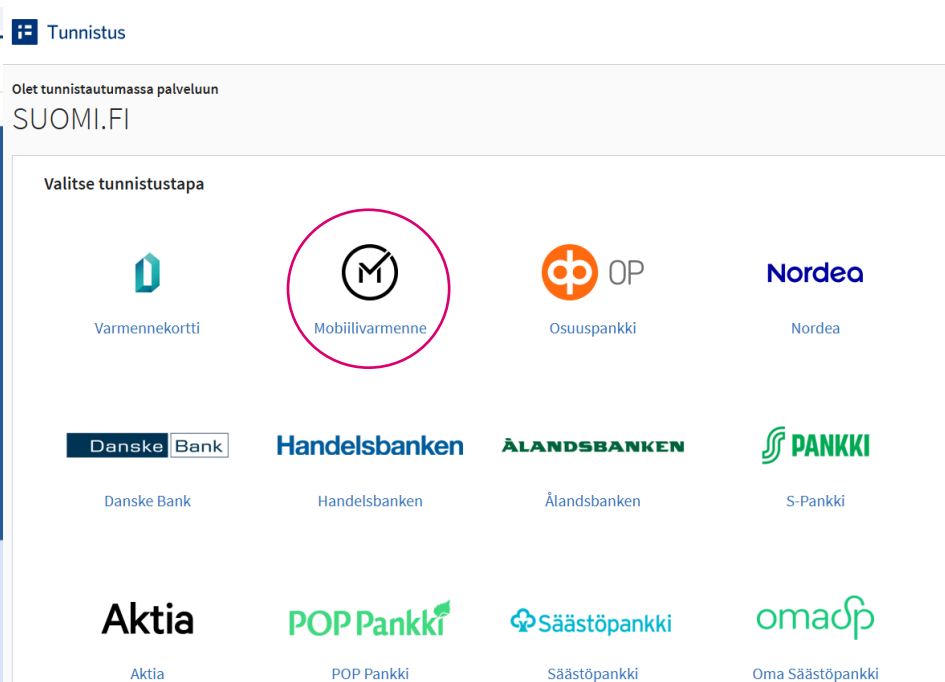
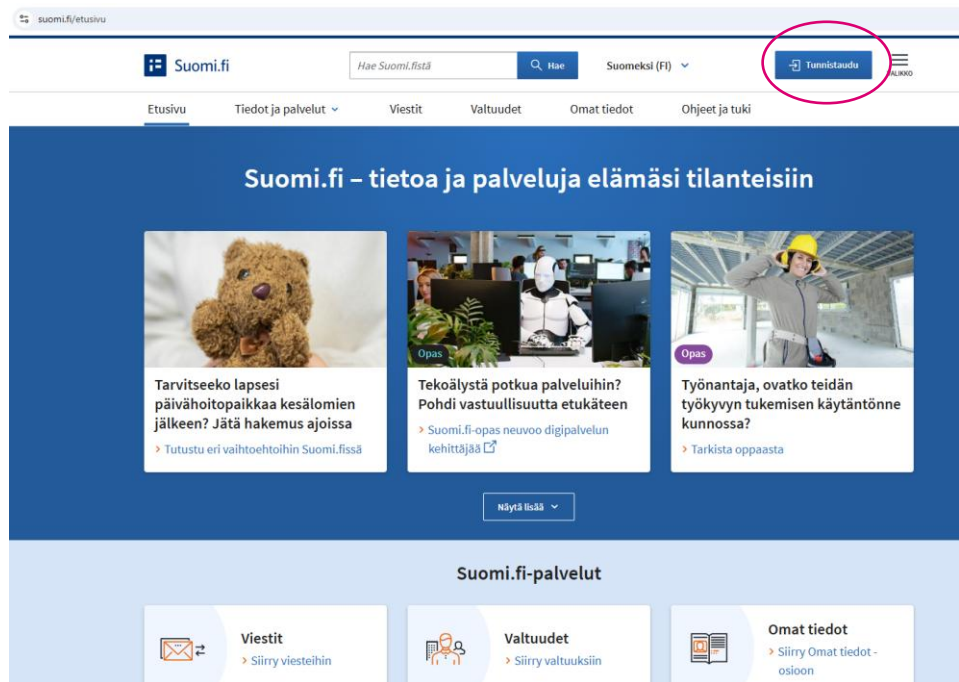
Miten Mobiilivarmennetta käytetään?

Miten tunnistaudun palveluissa Mobiilivarmenteella?

Miten käytän Mobiilivarmennetta? (esimerkki Suomi.fi-palvelu)

1. Mene palvelussa kohtaan
”Tunnistaudu” tai ”Kirjaudu”.

2. Valitse tunnistustavaksi
Mobiilivarmenne.



Miten käytän Mobiilivarmennetta?

3. Syötä oma puhelinnumero.

FI | SV | EN

 Telia

Tunnistaudu palveluun

Suomi.fi-tunnistus

Syötä puhelinnumerosi (esim. 0401234567)

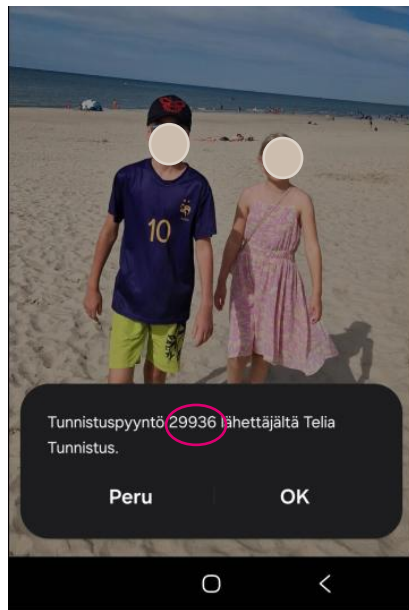
Puhelinnumero:

 Syötä puhelinnumerosi (esim. 0401234567)

KESKEYTÄ **JATKA**

Tämä asiointi on suojattu [Telia Tunnistus](#)-palvelun avulla.
Telian luottamuspalveluilla [allekirjoitat](#), [tunnistat](#), [varmennat](#) ja [arkistoit](#) luotettavasti.
[Asiakaspalvelun yhteystiedot](#) [Tietosuoja ja -turva](#)

4. Puhelimellesi tulee tunnistuspyyntö. Varmista, että tapahtumatunniste on sama kuin palvelun sivulla ja paina "OK".



Sensitivity: Internal

FI | SV | EN

 Telia

Tunnistautuminen käynnissä palveluun

Suomi.fi-tunnistus

Tunnistuspyyntö on lähetetty puhelimeesi. Tarkista ennen pyynnön hyväksymistä, että tapahtumatunniste ja puhelimeesi lähetetty numero ovat samat.

Puhelinnumero:

 +358440443224

Tapahtumatunniste:

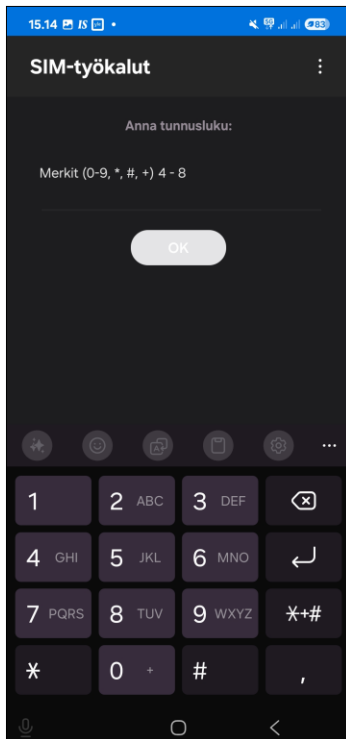
 29936

KESKEYTÄ

Tämä asiointi on suojattu [Telia Tunnistus](#)-palvelun avulla.
Telian luottamuspalveluilla [allekirjoitat](#), [tunnistat](#), [varmennat](#) ja [arkistoit](#) luotettavasti.
[Asiakaspalvelun yhteystiedot](#) [Tietosuoja ja -turva](#)

Miten käytän Mobiilivarmennetta?

5. Anna Mobiilivarmenteelle määrittämäsi tunnusluku.



6. Olet tunnistautunut palveluun ja voit jatkaa sen käyttöä.

Tunnistus

Olet tunnistautumassa palveluun

SUOMI.FI



Varmista tietoturvallinen käyttö

Kun lopetat palvelun käytön, muista kirjautua palvelusta ulos sen omilla sivuilla ja sulje selain.

Tunnistautumisen yhteydessä sinusta välitetään seuraavat tiedot:

Henkilötunnus:

Sukunimi:

Etunimet:

Jatka palveluun

Keskeytä siirtyminen



Tunnistautumiseen tarvittavat henkilötietosi on haettu väestötietojärjestelmästä. Voit tarkastaa omat tietosi Suomi.fi:n [Henkilötiedot](#) -sivulta.

Palvelu, johon olet tunnistautumassa, tarvitsee henkilötietosi asiointia varten. Löydät tiedon niiden käsittelystä, kun tunnistaudut palveluun.

Kun tunnistaudut yhteen Suomi.fi-tunnistusta käyttävään asiointipalveluun, voit siirtyä toisiin palveluihin 32 minuutin ajan ilman uutta tunnistautumista. Kun kirjaudut ulos yhdestä käyttämästäsi palvelusta, kirjaudut samalla ulos kaikista.

Kiitos!

Kysymyksiä?