



# Vahva sähköinen tunnistaminen pähkinänkuoressa

Laura Kolinen  
Ylitarkastaja

# Mitä vahva sähköinen tunnistaminen on?

- Vahvan sähköisen tunnistusvälineen avulla käyttäjät osoittavat turvallisesti henkilöllisyytensä, kun he käyttävät sähköisiä palveluja.
  - henkilöllisyyden todentaminen sähköisesti
- Lisäksi sähköiset asiointipalvelut voivat sähköisen tunnistamisen avulla tunnistaa asiakkaansa.
- Suomessa pankkitunnukset sekä teleoperaattoreiden mobiilivarmenne ovat yleisimpiä välineitä vahvaan sähköiseen tunnistautumiseen.



Varmennekortti



Mobiilivarmenne



Osuuspankki

Nordea

Nordea



Danske Bank

Handelsbanken

Handelsbanken

ÅLANDSBANKEN

Ålandsbanken

S-Pankki  
FIM

S-Pankki

Aktia

Aktia



POP Pankki



Säästöpankki

omaop

Oma Säästöpankki

*Esimerkki: tunnistautuminen suomi.fi-sivustolle, kuvakaappaus*

# Mikä tekee sähköisestä tunnistamisesta vahvaa?

- Vahva sähköinen tunnistus voi perustua teknisesti eri menetelmiin
- Menetelmän elementteinä on oltava vähintään kaksi alla olevista todentamistekijöistä:
  - Henkilön tiedossa oleva tekijä
    - esim. salasana, PIN-koodi
  - Henkilön hallussa oleva tekijä
    - esim. tunnuslukulaite, mobiilisovellus, tunnuslukulista
  - Luontainen tekijä
    - perustuu luonnollisen henkilön fyysiseen ominaisuuteen

# Mitä hyötyä vahvasta sähköisestä tunnistamisesta on?

- Digitalisoituva yhteiskunta: sähköisten palvelujen määrä ja kirjo lisääntyy
  - Tämä edellyttää myös yhä useammin luotettavaa sähköistä tunnistamista
- Avainasemassa vahvassa tunnistamisessa on sähköisten palvelujen käytön **turvallisuus** ja **luotettavuus**
  - Kuluttajan näkökulma
  - Asiointipalvelun näkökulma
- Verrokkina ns. heikot tunnistusmenetelmät (käyttäjätunnus + salasana)



# Miten vahvaa sähköistä tunnistamista on säännelty?

- Laki vahvasta sähköisestä tunnistamisesta ja sähköisistä luottamuspalveluista (617/2009)
- Lainsäädäntöä ja palveluita on Suomessa kehitetty pitkäjänteisesti markkinaehtoisuudelle perustuen.
- Laissa säädetään esimerkiksi
  - Tunnistusvälineen tietoturva-vaatimuksista
  - Tunnistusvälineen käyttäjän oikeuksista ja velvollisuuksista
  - Vahvan sähköisen tunnistamisen markkinoista (luottamusverkosto)
- EU:n eIDAS-asetus
  - Rajat ylittävä sähköinen tunnistaminen
  - Uudistustyö käynnistyy 2021



# Mitkä ovat vahvan sähköisen tunnistamisen kehityssuuntia?

- Vahvan sähköisen tunnistamisen käytön lisääntyminen
  - Tietosuoja- ja tietoturvaloukkaukset
  - Identiteettivarkaudet
- Luotettava sähköinen tunnistaminen – mutta ei vahva
  - Tilanteet, jotka eivät edellytä tietoa henkilöllisyydestä
- Tulevaisuuden tarpeita?
  - Anonymiteetti
  - Vain tietyn tiedon välittäminen ja henkilötietojen minimointi



# Kiitos!

[lvm.fi](http://lvm.fi) Twitter: [@lvmfi](https://twitter.com/lvmfi)

**LVM** LIIKENNE- JA  
VIESTINTÄMINISTERIÖ