



Liikenne- ja viestintävirasto
Kyberturvallisuuskeskus

Henkilön sähköinen tunnistaminen

Liikennemarkkinaverkoston
käytännösääntötyöpaja 30.10.2019

Henkilön sähköinen tunnistaminen

Motto: henkilötunnuksen kysyminen ei ole
tunnistamista



Henkilöllisyyden varmistamisen kolme osaa

1. Henkilön yksilöinti (identification)

- ▶ Millä tiedoilla henkilö erotetaan kaikista muista henkilöistä

2. Henkilöllisyyden todentaminen (verification/proofing of identity)

- ▶ Miten henkilö osoittaa olevansa tietty henkilö

3. Henkilön sähköinen tunnistaminen (authentication)

- ▶ Miten asiainnissa varmistetaan, että asioimassa on tietty henkilö
- ▶ Erotettava asioivan henkilön toimenpiteet ja sähköisen palvelun tarjoajan/tarjoajien toimenpiteet konepellin alla

1. Henkilön yksilöinti (identification)

- ▶ Millä tiedoilla henkilö erotetaan kaikista muista henkilöistä
- ▶ Ratkaistava, mikä on riittävä määrä henkilötietoja
 - ▶ Henkilötunnus ja nimi riittävät Suomessa yksilöimään väestötietojärjestelmään merkityt henkilöt
 - ▶ Jos ei käytetä henkilötunnusta, arvioitava, mikä muu tietojoukko riittää erottamaan henkilön muista henkilöistä
 - ▶ Nimi, entiset nimet, syntymäaika, syntymäpaikka, postiosoite, puhelinnumero, sähköpostiosoite, asiakasnumero, ...
- ▶ Mahdollisuus tarkistaa, ovatko henkilötiedot aitoja/olemassa
 - ▶ Väestötietojärjestelmä
 - ▶ Muut lähteet

Mitä
henkilötietoja
käytätte
käyttäjätilin ja
henkilön
yksilöinnissä
palvelussanne

2. Henkilöllisyyden todentaminen (verification/proofing of identity) - miten

- ▶ Miten henkilö osoittaa olevansa se henkilö, jonka henkilötiedot hän on kertonut
- ▶ **Henkilöllisyystodistus esitetään fyysisesti tai sähköisesti**
 - ▶ Virallinen kuvallinen henkilöllisyystodistus (passi, henkilökortti)
 - ▶ kuvan ja henkilön vertailu
 - ▶ Mahdollisesti etänä passin sirulta luetun kuvan sähköisen allekirjoituksen tarkastaminen ja kuvan vertailu etäyhteyden päässä olevaan esittäjään
- ▶ **Muu todistus esitetään fyysisesti tai sähköisesti**
 - ▶ kuvallinen tai kuvaton asiakirja/todistus, jossa henkilöllisyys ilmenee (ajokortti, ...)
 - ▶ mikä tahansa lähde, jonka luotetaan kansallisella tasolla tuottavan kelvollista tietoa
- ▶ **Sähköinen tunnistus**
 - ▶ Vahva sähköinen tunnistus
 - ▶ Muu sähköinen tunnistus (google, facebook...)

Miten
tunnistatte
henkilön,
kun luotte
hänelle
käyttäjätilin

2. Henkilöllisyyden todentaminen (verification/proofing of identity) – miten - jatkuu

▶ Henkilö kertoo itse erilaisia henkilötietojaan

▶ + tietojen tarkistaminen

- ▶ Tietojen määrä voi helpottaa todentamista
- ▶ Tiedot, joita ei voi olla muilla - aiemmin rekisteröity tieto ja tieto, joka on todennäköisesti vain henkilön omassa tiedossa
- ▶ henkilön tunnettuun osoitteeseen lähetettyihin asiakirjoihin sisältyviä tietoja, jotka eivät ole julkisia
- ▶ mikä tahansa lähde, jonka luotetaan kansallisella tasolla tuottavan kelvollista tietoa
- ▶ Tarkistaminen useista toisistaan riippumattomista tietolähteistä
- ▶ Henkilö osoittaa, että hänellä on hallussaan puhelinnumero
- ▶ Henkilö osoittaa, että hänellä on pääsy sähköpostitili
- ▶ Maksutapahtuma tms. - pääsy pankkitilille tai vastaavalle varmennetaan pyytämällä häntä tekemään maksutapahtuma, joka edellyttää pankkitilin käyttöä



Miten
tunnistatte
henkilön, kun
luotte hänelle
käyttäjätilin

2. Henkilöllisyyden todentaminen (verification/proofing of identity) - mihin

- ▶ Henkilöllisyyden varmistaminen tunnistusvälinettä/tokenia annettaessa ja ylläpito välineen elinkaaren aikana
- ▶ Henkilöllisyyden sitominen luotettavasti välineeseen/tokeniin
- ▶ Tunnistusvälineet/tokenit, esim.
 - ▶ Käyttäjätunnus
 - ▶ Mobiilisovellus
 - ▶ PIN/salasana
 - ▶ sormenjälki
 - ▶ Salasanalaite
 - ▶ salasanalista



Miten
tunnistatte
henkilön, kun
luotte hänelle
käyttäjätilin

3. Henkilön sähköinen tunnistaminen (authentication) - miten

Miten
tunnistatte
asiakkaan,
kun hän
asioi
käyttäjätilillä

- ▶ Miten asioinnissa varmistetaan, että asioimassa on tietty henkilö
- ▶ Käyttäjä asioi sillä menetelmällä ja niillä todentamistekijöillä, joihin hänen henkilöllisyytensä on kytketty
- ▶ Menetelmä voi perustua yhteen tai useampaan todentamistekijään (single factor, multifactor)
 - ▶ hallussapitoon perustava todentamistekijä, esim. sirukortti, salasanalista, mobiilisovellus, OTP-token, SMS-vahvistus
 - ▶ tiedossaoloon perustava todentamistekijä, esim. käyttäjätunnus, salasana/PIN-koodi, aiemmin rekisteröity tieto ja tieto, joka on todennäköisesti vain henkilön omassa tiedossa
 - ▶ luontainen todentamistekijä, esim. sormenjälki, kämmenjälki, kämmenen verisuonisto, kasvot, käden geometria ja silmän iiris

3. Henkilön sähköinen tunnistaminen (authentication) – konepellin alla

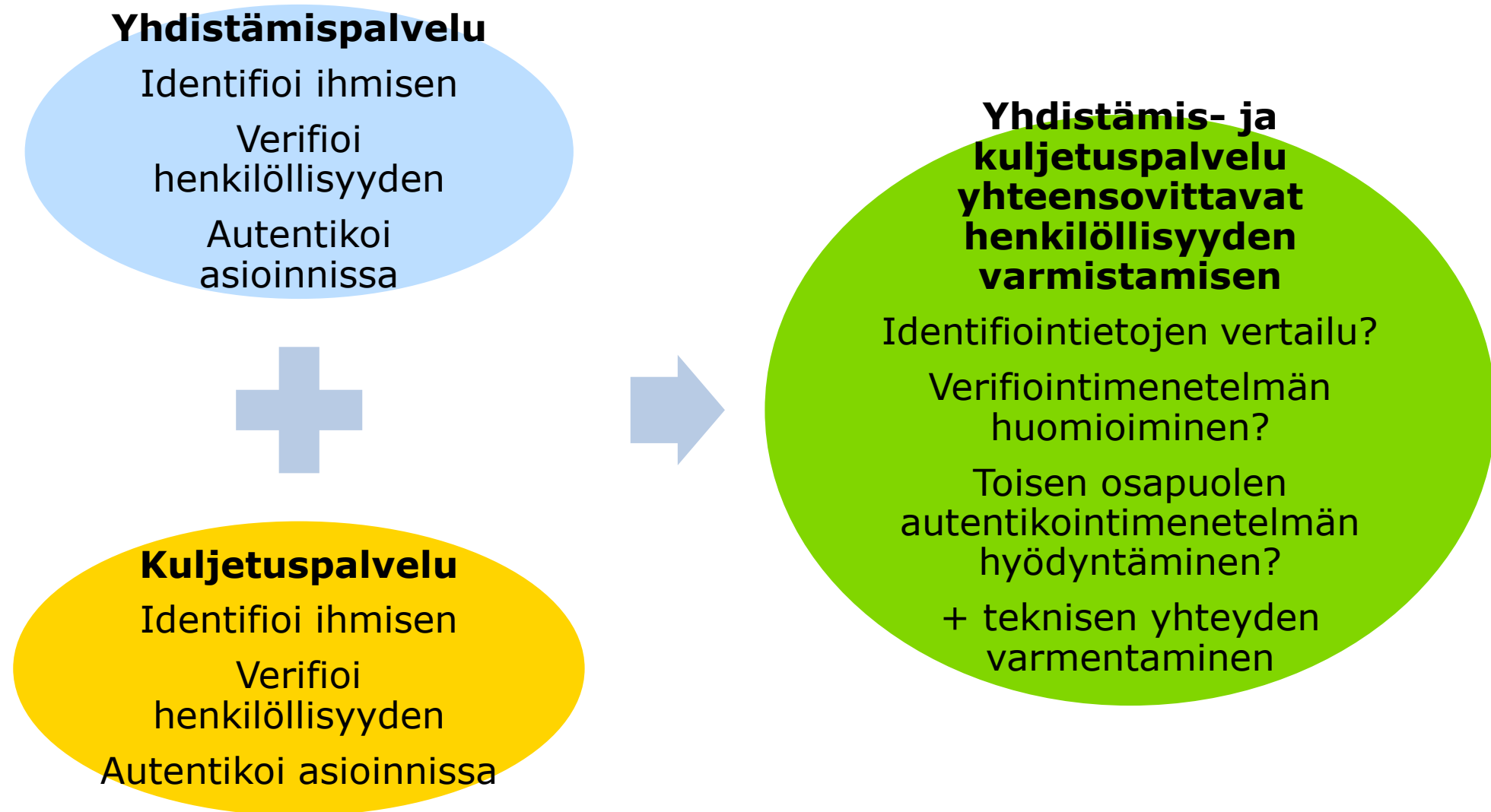
- ▶ Erotettava asioivan henkilön toimenpiteet ja sähköisen palvelun tarjoajan/tarjoajien toimenpiteet
- ▶ HE: ... *Teknisessä mielessä tähän voitaneen käyttää erilaisia ratkaisuja, kuten tunnisteita, varmenteita tai pseudonyymejä.*
- ▶ Esimerkit voivat liittyä henkilöllisyyden todentamiseen ja tunnistamiseen, mutta myös yhdistämispalvelun ja kuljetuspalvelun "tekniseen tunnistamiseen" tietoliikenteessä
- ▶ Varmenne:
 - ▶ Varmenne on aina yksityisen ja julkisen avaimen (eli PKI) käyttöön perustuva tapa. Pääsääntöisesti varmenteen myöntää ulkopuolinen taho eli varmentaja. Varmenteeseen luottaminen edellyttää siis varmentajaan luottamista.
 - ▶ Käyttäjän tunnistus varmenteella: yksityinen tunnistus- tai allekirjoitusavain on sirukortilla tai mobiililaitteessa (hallussapito), jonka käyttäjä avaa omalla PIN-koodillaan (tieto). Yksityisellä avaimella allekirjoitetaan tunnistusta pyytävän tahon lähettämä haaste. Tunnistusta pyytävä taho tarkistaa allekirjoitetun haasteen ja henkilön varmenteen henkilön julkisella avaimella.
 - ▶ Yhdistämispalvelun tunnistus varmenteella: varmistetaan, että kuljetuspalvelun ja yhdistämispalvelun tietoliikenne kulkee oikeiden osapuolten välillä. Tässä voi tyypillisesti käyttää osapuolten varmenteita.

3. Henkilön sähköinen tunnistaminen (authentication) – konepellin alla jatkuu

- ▶ Tunniste/pseudonyymi:

- ▶ Tietoja, jotka jompikumpi puolesta-asioinnin osapuoli määrittelee/luo
- ▶ käytöstä täytyy sopia, jotta voi liittyä kuljetuspalvelussa ja yhdistämispalvelussa saman henkilön asiointiin
- ▶ Henkilötietosäätelyn kannalta tunnisteet, jotka ovat liitettävissä henkilöön, ovat pseudonyymejä
- ▶ Esim. sähköisten rajapintojen standardien tokenit
- ▶ Tunnisteiden/pseudonyymien käyttö parantaa henkilötietojen suojaa

Henkilöllisyyden varmistamisen yhteensovittaminen



Liikennepalvelulain näkökulma

Henkilöllisyyden varmistamisen
turvallisuuustaso

Tunnistaminen, tietoturva ja tietosuoja liikennepalvelulain näkökulmasta

- ▶ Puolesta-asioinnissa käsitellään henkilötietoja
 - ▶ HE: ...asiointitapahtuman yhteydessä on voitava varmistua siitä, että kyse on oikean henkilön asiakas- tai käyttäjätilin tietojen hyödyntämisestä.
- ▶ Henkilötietojen suojasta ei voi huolehtia ilman tietoturvallisuutta
- ▶ Asiakkaan henkilöllisyyden varmistaminen on osa tietoturvallisuutta
- ▶ Varmistamisen taso – kuten muukin tietoturvallisuus- on suhteutettava uhkiin, niiden vakavuuteen ja todennäköisyyteen.
- ▶ Liikennepalvelulaissa ja sen perusteluissa määritellään yleiset suuntaviivat varmistamisen tasolle.

Tunnistaminen, tietoturva ja tietosuoja liikennepalvelulain näkökulmasta - otteet

- ▶ *...rajapintojen avaamiseen velvoitettujen palveluntarjoajien on huolehdittava siitä, että avaaminen voi tapahtua palvelun tietoturvan ja yksityisyyden suojan vaarantumatta.*
- ▶ *...pääsyyn oikeutetun liikkumis- tai yhdistämispalvelun tarjoajan on huolehdittava oman palvelunsa tietoturvan ja tietosuojan tasosta niin, että puolesta-asiointi voi tapahtua näitä vaarantamatta.*
- ▶ *Henkilötietoja saa käsitellä puolesta-asiointitapahtumassa ainoastaan siinä määrin kuin on tarpeen henkilöllisyyden varmistamiseksi ja puolesta-asiointitapahtuman toteuttamiseksi.*
- ▶ *Pääsyn käyttäjätilin tietoihin on oltava riittävän laaja, jotta liikkumis- ja yhdistämispalvelun tarjoajat voivat tarjota palvelujaan esteettä ja tehokkaasti.*
- ▶ *Huolehdittava siitä, että alennuksen, korvauksen tai erityisehdon määräytymisperusteeseen liittyvät tiedot ovat käytettävissä siinä määrin kuin on tarpeen puolesta-asiointitapahtuman toteuttamiseksi.*

GDPR 32 [henkilötietojen] Käsittelyn tietoturvallisuus – riskit ja toimenpiteet - otteet

► Otettava huomioon

- *luonnollisten henkilöiden oikeuksiin ja vapauksiin kohdistuvat riskit*
- *vahingossa tapahtuva tai laitton tuhoaminen, häviäminen, muuttaminen, luvaton luovuttaminen tai luvaton henkilötietoihin pääsy*

► rekisterinpitäjän on toteutettava

- *riskiä vastaavan turvallisuustason varmistamiseksi asianmukaiset tekniset ja organisatoriset toimenpiteet, kuten*
- *henkilötietojen pseudonymisointi ja sala*us
- *kyky taata käsittelyjärjestelmien ja palveluiden jatkuva luottamuksellisuus, eheys, käytettävyys ja vikasietoisuus*
- ...



TRAFICOM

Liikenne- ja viestintävirasto
Kyberturvallisuuskeskus