| Jakelun mukaan |
| --- |

Poliisihallituksen lausunto luonnoksesta hallituksen esitykseksi digitaalista henkilöllisyyttä koskevaksi lainsäädännöksi

Valtiovarainministeriö on lähettänyt Poliisihallitukselle lausuttavaksi luonnoksen hallituksen esitykseksi digitaalista henkilöllisyyttä koskevaksi lainsäädännöksi. Hallituksen esityksessä ehdotetaan säädettäväksi laki Digi- ja väestötietoviraston digitaalisen henkilöllisyyden palveluista sekä laki digitaalisesta henkilöllisyystodistuksesta. Lisäksi vahvasta sähköisestä tunnistamisesta ja sähköisistä luottamuspalveluista annettua lakia, väestötietojärjestelmästä ja Digi- ja väestötietoviraston varmennepalveluista annettua lakia, henkilötietojen käsittelystä poliisitoimessa annettua lakia, henkilökorttilakia, passilakia sekä hallinnon yhteisistä sähköisen asioinnin tukipalveluista annettua lakia ehdotetaan muutettavaksi.

Ehdotuksella on tarkoitus mahdollistaa digitaalisen henkilöllisyystodistuksen sekä ulkomaalaisen digitaalisen asiointivälineen tuottaminen ja käyttö. Kyse olisi uusista digitaalista asiointia tukevista mobiilisovelluksista, joita poliisi ja Digi- ja väestötietovirasto tuottaisivat vahvistettujen henkilötietojen osoittamiseksi. Digitaalinen henkilöllisyystodistus toimisi myös henkilöllisyyttä osoittavana asiakirjana. Esityksen yhtenä erityisenä tavoitteena on rakentaa edellytyksiä henkilön itsensä toimesta tapahtuvaan henkilöön itseensä liittyvien viranomaisten vahvistamien tietojen jakamiseen (ns. itsehallittava identiteetti, Self-sovereign identity). Tavoitteena on ensivaiheessa mahdollistaa tiettyjen henkilöllisyyttä koskevien tietojen esittäminen henkilön itsensä toimesta, sekä luoda pohjarakenteet ja käytännöt itsehallittavien viranomaistietojen esittämiseksi, jotta kehitystä voidaan viedä eteenpäin tulevaisuudessa. Lakiehdotukset on tarkoitettu tulemaan voimaan 1.1.2023.

Poliisihallitus on osallistunut aktiivisesti digitaalista henkilöllisyyttä koskevien muutosten valmisteluun ja jakaa hallituksen esityksen luonnoksessa esitetyt peruslähtökohdat. Lausuntopalvelu.fi verkkopalvelussa on esitetty joukko kysymyksiä, joihin lausunnonantajia on pyydetty vastaavan. Poliisihallituksen lausunto on pyritty laatimaan siten, että se vastaa soveltuvin osin esitettyihin kysymyksiin.

# Esitysluonnos

Hallituksen esitysluonnoksessa esitetty kokonaisuus on laaja ja sisältää monin osin uudenlaisia digitaalisen ympäristön toimintatapoja. Kokonaisuus on osin vaikeasti hahmotettava eikä esityksestä ole kovin helppo saada yksiselitteistä kuvaa siitä, mitä konkreettisella tasolla digitaalisen henkilöllisyyden käyttämisen eri vaiheissa tapahtuu. Digitaalisen henkilöllisyystodistuksen elinkaaren eri vaiheiden tarkempi kuvaaminen sekä tähän liittyvät tiedonsiirrot olisi tärkeä voida avata yksiselitteisesti hallituksen esityksessä.

## Jatkovalmistelu

Poliisihallitus nostaa esiin huolensa lainsäädäntöhankkeen jatkovalmistelusta. Jo lausuntokierroksen aikana on valmistelevien viranomaisten käyty jatkokeskustelua tarvittavista muutoksista, joita ei ole hallituksen esityksessä huomiota ja jotka ovat merkittäviä kokonaisuuden näkökulmasta. Hankkeen aikataulu on erittäin kiireinen eikä jatkovalmistelulle voida varata siihen tarvittavaa aikaa. Myöskään ei ole täysin ongelmatonta, jos muutokset tulevat olemaan niin laajoja, ettei lausunnolla oleva luonnos vastaa perusratkaisultaan lopullista hallituksen esitystä.

## Aikataulu

Hallituksen esitysluonnoksen mukaisesti muutokset on suunniteltu tulevan voimaan vuoden 2023 alusta. Ottaen huomioon sen, ettei säädöksen lopullinen muotoilu ole käytännössä selvillä vasta kuin vuoden 2022 lopulla, voidaan esitettyä voimaantuloajankohtaan 1.1.2023 pitää erittäin tiukkana.

Esitetty toiminta tulee sisältämään mm. laajamittaista Suomen kansalaisten ja osin ulkomaalaisten henkilötietojen ml. kasvokuvatietojen käsittelyä, mistä syystä on esityksessäkin nähty tarpeelliseksi todeta tietosuojaa koskevan vaikutusten arvioinnin toteuttaminen. On hyvä huomata tietosuojaa koskevan vaikutustenarvioinnin, sisältäen mahdollisen ennakkokuulemisen, vievän joitain kuukausia aikaa. Myös esitetyn järjestelmän käyttöönotto edellyttää normaalin käyttöönottokäsittelyn, johon kuuluu käyttöönottoprosessin läpikäyminen ennen käyttöönottopäätöstä.

Lisäksi tiedonhallinnan näkökulmasta tuodaan esille, että asiaan liittyen olisi syytä tarkastella uudelleen vuonna 2020 tehty muutosvaikutusten arviointi, joka perustuu julkisen hallinnon tiedonhallinnasta annettuun lakiin ((906/2019) tiedonhallintalaki), peilaten sitä nyt esitettyyn. Digitaalisen henkilöllisyystodistukseen liittyen tulee poliisissa perustettavaksi uusi tietovaranto, jossa on ulkoisia yhteyksiä ja rajapintoja. Lisäksi uusi toiminto luo muutoksia nykyisiin prosesseihin sekä mahdollisesti myös nykyiseen tiedonohjaussuunnitelmaan (TOS) ja tiedonhallintamalliin.

Edellä mainitut tarkastelut ja mahdolliset muutokset, tietosuojaa koskeva vaikutustenarviointi, käyttöönottokäsittelyt, muutosvaikutusten arvioinnin päivittäminen sekä mahdolliset tietojen korjaamiseen, poistamiseen ja valvontaa liittyvien toimien rakentamista ei välttämättä ole mahdollista toteuttaa esitetyssä aikataulussa.

# Digitaalinen henkilöllisyystodistus

Digitaalinen henkilöllisyystodistus on Suomen kansalaiselle ja Suomessa oleskelevalle ulkomaalaiselle myönnettävä digitaalinen asiakirja, jolla henkilöllisyys ja siihen liittyviä vahvistettuja tietoja voitaisiin osoittaa, ja jonka henkilö voisi saada käyttöönsä, kun hänellä on voimassa oleva suomalainen passi tai henkilökortti. Välinettä voidaan käyttää sekä sähköisessä tunnistamisessa että käyntiasioinnissa.

## Digitaalisen henkilöllisyystodistuksen kokonaisturvallisuus

Poliisille sisäisen turvallisuuden keskeisenä viranomaisena on elinarvoisen tärkeää, että sen tarjoamat viranomaistoiminnot ovat mahdollisimman korkealla turvallisuustasolla eikä tehtävillä valinnoilla mahdollisteta rikollista väärinkäyttöä. Digitaalinen henkilöllisyystodistus pitää sisällään sekä sähköiseen asiointiin tarkoitetun tunnistusvälineen, että fyysiseen asiointiin tarkoitetun digitaalisessa muodossa olevan henkilöllisyystodistuksen. Näiden toteutus nivoutuu yhteen, mutta niiden turvatasoa koskeva sääntely poikkeaa toisistaan olennaisesti.

Hallituksen esityksen luonnoksessa on selkeästi säännelty turvallisuustasosta, jolle tunnistusjärjestelmää koskevat vaatimukset asettuvat. Lain DVV:n digitaalisen henkilöllisyyden palveluista 6 §:n mukaan on tunnistamisjärjestelmän täytettävä vähintään eIDAS korkea tai korotettu tason vaatimukset. Käyntiasiointia koskeva toiminnallisuuden osalta vastaavaa sääntelyä ei ole hallituksen esityksen luonnoksessa. Keskeisenä ongelmana sääntelyn valmistelun näkökulmasta on luonnollisesti se, että käyntiasiointiin tarkoitetut digitaaliset välineet ovat siinä määrin uutta teknologiaa, ettei niihin ole vakiintunut vastaavia arviointikriteerejä kuin sähköisen asioinnin osalta on erityisesti eIDAS.

Tästä huolimatta Poliisihallitus tunnistaa tarpeen säännellä tarkemmin digitaalisen henkilöllisyystodistuksen kokonaisturvallisuudesta siten, että myös käyntiasiointia koskevien ratkaisujen turvallisuus tulee selkeästi huomioiduksi. On ehdottoman tärkeää, että digitaalisen henkilöllisyystodistuksen turvallisuustaso vastaa kokonaisuudessaan sitä hyvin korkeaa turvallisuuden tasoa, jolla sen perustana olevat fyysiset henkilöllisyyttä osoittavat asiakirjat ovat. Tästä näkökulmasta on jokseenkin haasteellista, ettei esityksessä ole lähdetty liikkeelle eIDAS korkea tasolle asettuvasta tunnistamisjärjestelmästä.

## Digitaalisen henkilöllisyystodistuksen tietosisältö

Laissa digitaalisesta henkilöllisyystodistuksesta 5 §:ssä on määritelty kyseisen välineen tietosisältö. Säännösehdotuksen mukaan digitaalisen henkilöllisyystodistuksen haltijalle toimitettaisiin kopio häneen liittyvistä henkilökorttilain (663/2016) 31 §:ssä tarkoitetun henkilökorttirekisterin tai passilain (671/2006) 29 §:ssä tarkoitetun passirekisterin sisältämistä tiedoista hänen itsensä hallittavaksi.

Hallituksen esityksen perustelujen mukaan digitaalinen henkilöllisyystodistus sisältäisi momentissa yksilöidyt luonnollisen henkilön tiedot sellaisina, kuin ne sisältyvät henkilökorttirekisteriin tai passirekisteriin. Digitaalisen henkilöllisyystodistuksentietojen lähderekisteri riippuisi alkuperäisestä digitaalisen henkilöllisyystodistuksen käyttöönottoon perustuvasta viranomaisen henkilöllisyyttä osoittavasta asiakirjasta, eli kyse olisi joko passirekisterin tiedoista henkilön ottaessa todistuksen käyttöön passilla tai henkilökorttirekisterin tiedoista henkilön ottaessa todistuksen käyttöönsä henkilökortilla.

Esitetty lähtökohta on osittain ristiriidassa saman pykälän 5 §:n 3 momentin perusratkaisun kanssa. Kyseisen säännöksen mukaan Digitaalisen henkilöllisyystodistuksen käytön edellytyksenä on, että sen sisältämät tiedot ovat aina ajan tasalla ja vastaavat poliisin 1 momentin rekistereissä olevia tietoja. Säännöksen tarkoituksena on, että digitaalisen henkilöllisyystodistuksen tulee sisältää aina ne passi- tai henkilökorttirekisterissä olevat henkilötiedot, jotka ovat tuoreimmat.

5 §:n 1 momentin perusteluissa esitetyn mallin mukaan käyttöönoton yhteydessä tietojen lähde ei määrittyisi sen rekisterin perusteella, jossa on tuoreimmat tiedot vaan sen perusteella, mitä asiakirjaa käyttöönoton yhteydessä on esitetty. Koska henkilöllisyysasiakirjat eivät lain mukaan raukea tilanteessa, jossa henkilötiedot muuttuvat, esiintyy käytännössä tilanteita, joissa henkilöllä on sekä voimassa oleva passi, että henkilökortti, joissa on toisistaan eroavat henkilötiedot. Esimerkiksi voi syntyä tilanne, jossa henkilöllä on henkilökortti vanhalla nimellä ja passi uudella nimellä ja hän käyttää henkilökorttia välineen käyttöönottamiseen omatoimisesti. Lain 5 § 1 mom logiikan mukaan digitaaliseen henkilöllisyystodistukseen tulee henkilökortin tiedot, mutta samaisen pykälän 3 momentti edellyttäisi, että välineessä on tuoreimmat tiedot eli ne, jotka ovat passilla. Tästä syystä olisi järkevin, että myös käyttöönoton yhteydessä digitaaliseen henkilöllisyystodistukseen liitetään henkilötiedot passirekisteristä tai henkilökorttirekistä sen mukaan, missä on tuoreimmat tiedot. Käyttöönoton yhteydessä esitettävän passin tai henkilökortin tehtävänä on vahvistaa käyttäjän tunnistamista eikä sen suoraan tulisi määritellä digitaalisessa henkilöllisyystodistuksessa esitettävää tietosisältöä.

HE-luonnoksen mukaan digitaalisen henkilöllisyystodistuksen haltijalle toimitettavia tietoja olisivat seuraavat henkilötiedot: 1) etunimet; 2) sukunimi; 3) syntymäaika; 4) tieto henkilön sukupuolesta; 5) tieto Suomen kansalaisuudesta; 6) henkilötunnus tai muu kansallisen tason yksilöintitunnus; 7) passi- tai henkilökorttirekisteriin talletettu kasvokuva; sekä 8) voimassa olevan suomalaisen passin tai henkilökortin voimassaoloaika. Tämän lisäksi Digi- ja väestötietovirasto toimittaa syntymäajasta johdetut ikätodisteet digitaalisen henkilöllisyystodistuksen haltijalle.

Poliisihallitus katsoo, että digitaalisen henkilöllisyystodistuksen tulisi sisältää yllä esitettyjen lisäksi myös erillinen kyseisen välineen yksilöivä tunnus samaan tapaan kuin passissa ja henkilökortissa on asiakirjan numero. Tunnuksen tulisi olla määritelty siten, että se yksilöi myös sen laitteen, johon digitaalinen henkilöllisyystodistus on asennettu. Tunnuksen tarve liittyy siihen, että varsinkin toteutuksen alkuvaiheessa ainoana käyntiasioinnin muotona toteutettavan mobiililaitteessa käytettävän tarkastussovelluksen käytön yhteydessä on henkilöllisyyden tarkastaminen oltava osoitettavissa jälkikäteisesti kiistattomalla tavalla.

Yksinkertaisemmin todettuna yllä mainitulla tarkoitetaan tilanteita, joissa nykyisin tunnistustapahtuman yhteydessä otetaan ylös henkilöllisyyden osoittamiseen käytetyn lupa-asiakirjan numero, jotta jälkikäteen voidaan kiistatta todeta, millä tavoin henkilö on asiointitapahtuman yhteydessä tunnistettu. Esimerkiksi tällainen prosessi on käytössä poliisin myöntämien passien ja henkilökorttien suoratoimitusprosessissa, jossa yksityistä palveluntuottajaa käytetään asiakirjojen jakeluun. Prosessin turvallisuuden näkökulmasta on yhtenä monista vaatimuksista se, että lupa-asiakirjan numero talletetaan ja siten edellytyksenä digitaalisen henkilöllisyystodistuksen käyttöönottamiselle kyseisessä prosessissa on, että se sisältää välineen yksilöivan tunnuksen. Poliisilla on myös muita vastaavia käyttötapauksia ja varmasti monilla muilla viranomaisilla sekä yksityisillä toimijoilla on myös vastaavia käyttötapauksia.

Myöhemmin käyttöönotettavassa rajapintaratkaisussa, jossa tarkastaja käy tarkistamassa tietojen ajantasaisuuden DVV:n tarjoaman palvelun kautta, vastaava henkilöllisyyden osoittamisen jälkikäteinen tarkastaminen saattaa olla mahdollista toteuttaa jonkinlaisen lokituksen kautta, vaikka todennäköisemmin se on myös tässä käyttötapauksessa helpompi toteuttaa asiakirjan yksilöivän tunnuksen kautta.

## Digitaalisen henkilöllisyystodistuksen myöntäminen

Hallituksen esityksen luonnos on kirjoitettu sellaiseen muotoon, että oikeus digitaalisen henkilöllisyystodistukseen sisältyy voimassaolevaan passiin ja henkilökorttiin sekä sellaiseen ilman huoltajan suostumusta myönnettyyn alaikäisen henkilökorttiin, jonka haltija on yli 15-vuotias. Poliisi toimii muodollisesti välineen myöntäjänä, mutta erillistä hallintopäätöstä ei ole tarkoitus tehdä, vaan väline voidaan ottaa myönnetyn passin tai henkilökortin perusteella, kun käyttäjä noudattaa käyttöönotossa edellytettävä tunnistamismenettelyä.

Digitaalisen henkilöllisyystodistuksen käyttöönotossa on kyse ensisijaisesti välineeseen oikeutetun henkilön omaan aktiivisuuteen perustuvasta toimenpiteestä, jolla hän aktivoi passia tai henkilökorttia koskevassa myöntöpäätöksessä hänelle syntyneen oikeuden välineen käyttöön.

Luonnoksessa hallituksen esitykseksi päätöksentekoa koskeva seikka on tuotu esiin ainoastaan henkilökorttilain ja passilain muutoksia koskevissa yksityiskohtaisissa perusteluissa. Tämä pitäisi tuoda selkeästi esiin laissa digitaalisesta henkilöllisyystodistuksesta, jossa säännellään digitaalisesta henkilöllisyystodistuksesta ja sen käyttöönotosta. Ehdotetussa laissa digitaalisesta henkilöllisyystodistuksesta on nimenomaan todettu, että kyseessä on poliisin myöntämä väline. Myöntäminen terminä viittaa yleisesti menettelyyn, joka sisältää vähintäänkin jonkinasteista päätöksentekoa. Järjestely ei istu luontevalla tavalla hallinnollista päätöksentekoa koskevaan sääntelyyn. Sääntelyssä olisi tuotava selkeästi esiin, ettei kyseessä ole uuden luvan myöntäminen eikä poliisille synny velvoitetta päätöksen tekemiseen digitaalisen henkilöllisyystodistuksen käyttöönotosta. Selkeintä olisi, ettei sääntelyssä käytettäisi lainkaan termiä myöntää. Tällöin tulisi selkeämmin esiin perusajatus, että käyttöönotto tarkoittaa tilannetta, jossa henkilö omatoimisesti tai viranomaisen avustamana hyödyntää passin tai henkilökortin myöntöpäätöksen perusteella saamaansa oikeutta digitaalisen henkilöllisyystodistuksen käyttöönottoon.

Selkeyden vuoksi perusteluissa olisi syytä tuoda esiin myös se, ettei digitaalisen henkilöllisyystodistuksen saamiseksi ole muita edellytyksiä. Näin ollen käytännössä ei voi tulla eteen tilannetta, että jollekin ei kyseistä välinettä myönnettäisi.

Toinen asia on sitten tietenkin mahdolliset ongelmat sovelluksen toimimisesta esimerkiksi tietyissä mobiililaitteissa, mikä estää välineen käyttöönoton. Tällaisessa tapauksessa ei ole kuitenkaan viranomaisten harkintavaltaan kuuluvasta myöntämiseen liittyvästä asiasta. Esityksessä olisi kuitenkin tarpeen todeta, mikä on käyttöönottoa yrittävän henkilön oikeusasema tilanteessa. Onko hänellä esimerkiksi mahdollisuudesta hakea muutosta tällaisissa tilanteissa, joissa henkilöllisyystodistusta ei voida myöntää esim. puutteellisen tai syystä tai toisesta epäonnistuneen tunnistamisen vuoksi.

### Alaikäisten asiointi

Yksittäisenä asiakasryhmänä, jonka asiointitarpeella voi olla vaikutus poliisin toimintaan on alaikäiset. Sääntelyn tarkoituksena on perustelujen mukaan se, että kaikilla passin tai matkustusoikeudellisen henkilökortin omaavilla on ikään katsomatta oikeus välineen käyttöönottoon. Eli alaikäisillä olisi myös itsenäinen oikeus asioida poliisin luona välineen käyttöönottamiseksi.

Digitaalisen henkilöllisyystodistuksen myöntäminen on hallintomenettelyä ja siihen sovelletaan yleislakina hallintolakia siltä osin kuin erityislaissa ei säännellä menettelystä tarkemmin. Hallintolain yleisenä lähtökohtana on, että huoltaja käyttää puhevaltaa hallintoasiassa alaikäisen puolesta lisäksi viisitoista vuotta täyttäneellä alaikäisellä ja hänen huoltajallaan tai muulla laillisella edustajallaan on kummallakin oikeus erikseen käyttää puhevaltaa asiassa, joka koskee alaikäisen henkilöä taikka henkilökohtaista etua tai oikeutta.

Sääntelyssä olisi syytä täsmentää lainsäätäjän tarkoitusta. Mikäli on tarkoitus, että poiketaan hallintolain yleisestä puhevaltaa koskevasta säännöstä, jossa huoltaja käyttää puhevaltaa alaikäisen puolesta, olisi tästä säänneltävä selkeästi. Nyt esitetty sääntely tarkoittaa sitä, että hallintoasiaa, eli välineen käyttöönottoa koskevaa asiaa hoitaa ensisijaisesti alaikäisen huoltaja eikä alaikäinen itse, kuten esimerkiksi passi tai henkilökorttiprosessissa. Tästä poikkeuksena on alaikäisen henkilökortti, jonka osalta on erikseen säännelty, että alaikäinen voi itsenäisesti hoitaa siihen liittyvän hallintoprosessin.

Toisaalta Poliisihallitus tunnistaa, että täysin ikärajaton ratkaisu johtaa vääjäämättä erittäin haastaviin asiakaspalvelutilanteisiin, koska se mahdollistaa, että hyvinkin pienet lapset voivat saapua poliisin luokse ja hoitaa digitaalisen henkilöllisyystodistuksen käyttöönoton ilman huoltajan myötävaikutusta. Vaikka poliisi myöntää nykyiselläänkin alaikäisen henkilökorttia, joka on ilman huoltajan suostumusta myönnettävä henkilökortti, ei poliisin henkilöstöllä ole kattavaa koulusta tai osaamista siitä, miten itsenäisesti asioivan hyvin pienten alaikäisten lasten asiointitilanteet tulisi hoitaa. Ongelmalliseksi tilanteen tekee vielä se, että digitaalinen henkilöllisyystodistus on tekninen ratkaisu, jonka merkityksen ja toimintalogiikan ymmärtäminen vaatii kykyä ymmärtää monimutkaisia kokonaisuuksia.

### Alaikäiset ja tunnistusväline

Poliisihallitus haluaa tuoda esiin alaikäisten tunnistusvälineisiin ja niiden turvallisuuteen liittyvät riskit tässä yhteydessä. Esitettyjen muutosten tarkoituksena on mahdollistaa nykyistä kattavammin myös hyvinkin nuorten alaikäisten henkilöiden sähköinen asiointi.

Alaikäisten sähköistä asiointia on koettu tarpeelliseksi edistää etenkin opetus- ja terveydenhuoltoaloilla. Nykyisellään alaikäisten mahdollisuudet saada sähköisen asioinnin välineitä käyttöönsä eivät ole yhtä laajat kuin täysi-ikäisillä. Kansalaisvarmenne on ainoa sähköisen asioinnin väline, joka voidaan myöntää hakijan iästä riippumatta. Kansalaisvarmenne ei ole kuitenkaan saavuttanut suurta suosiota, koska sen käyttöä on pidetty haastavana.

Nyt esitettyjen muutosten tarkoituksena on, että hyvinkin pienet lapset voisivat ottaa oma-aloitteisesti käyttöön digitaalisen henkilöllisyystodistuksen ja myös siihen sisältyvän sähköisen asioinnin välineen. Alaikäisille myönnettyihin välineisiin liittyy kuitenkin olennaisia tunnistamisen luotettavuuteen liittyviä tekijöitä, jotka voivat lisätä olennaisella tavalla väärinkäytöksiä ja epäluottamusta etenkin alaikäisille myönnettyihin sähköisiin tunnistusvälineisiin.

Sähköisen tunnistusvälineen turvallisuus perustuu yhtäältä välineen tekniseen turvallisuuteen ja toisaalta luottamukseen siihen, että välineen haltija haluaa ja hänellä on kyky noudattaa hänelle asetettuja velvollisuuksia. Velvollisuuksista olennaisimpana se, ettei välinettä luovuteta toisen haltuun ja että siitä tulee pitää hyvää huolta. Jos väline ja siihen liittyvä salasana tai muu salainen elementti paljastuu tai luovutetaan toiselle, ei palvelun tarjoajalla ole mitään mahdollisuutta arvioida kuka todellisuudessa palvelussa asioi. Kun luottamussuhde rikotaan välineen käyttäjän päästä, ei palveluntarjoajalla ole mahdollista havaita sitä. Tämä luonnollisesti mahdollistaa välineen väärinkäytön myös rikollisiin tarkoituksiin. Tästä syystä käyttäjälle on usein asetettu suhteellisen ankara vastuu välineellä tehdyistä oikeustoimista, jos välinettä ei ole ilmoitettu kadonneeksi.

Sähköisen tunnistusvälineen kanssa toimittaessa ei voida koskaan täysin varmistua siitä, kuka välinettä käyttää. Perinteisissä tunnistusvälineissä kuten passissa tai henkilökortissa tunnistaminen perustuu nimenomaan siihen, että kyseessä oleva luonnollinen henkilö tunnistetaan, kun taas sähköisessä asioinnissa toiminta perustuu hyvin pitkälle luottamukseen suhteessa välineen haltijaan.

Mitä nuorempi sähköisen asioinnin välineen haltija on, sitä haastavampaa on luottaa siihen, että välineen haltija osaa toimia hänelle asetettujen velvoitteiden mukaisesti. Ensinnäkään nuoremmilla henkilöillä ei ole välttämättä riittävää kyky ymmärtämään välineen tarkoitusta ja mitä sillä voi tehdä. Toisaalta käyttäjällä ei ole myöskään usein tosiasiallisia mahdollisuuksia huolehtia välineestä ja sen turvallisesta säilyttämisestä. Voidaan perustellusti olettaa, että lähes kaikki alle 10-vuotiaiden ja suurin osa alle 15-vuotiaiden tekemistä tunnistautumisista on todellisuudessa jonkun toisen, eli useimmiten huoltajan, tekemiä.

On myös alaikäisten oikeusaseman näkökulmasta jokseenkin ongelmallista, että ehdotetun lain on mitä ilmeisimmin tarkoitus asettaa ankara vastuu välineen käytöstä myös kaikkein nuorimmille käyttäjille, jos välinettä ei ole asianmukaisesti ilmoitettu kadonneeksi. Käytännössä siis alaikäinen olisi vastuussa tehdyistä oikeustoimista tilanteessa, jossa hänen huoltajansa käyttävät välinettä ilman lupaa huollettavan sijasta.

Poliisihallitus katsoo, että kaikkein nuorimpien käyttäjien osalta mahdollisuutta ottaa digitaalinen henkilöllisyystodistus käyttöön olisi ehkä syytä rajata. Alaikäisten oikeus hoitaa asioita itsenäisesti on myös käytännössä hyvin rajattu lainsäädännössä. Itsenäinen oikeus koskee ainoastaan yksittäisiä opetustoimeen ja terveydenhuoltoon liittyviin lakeihin, joissa intressinä on tarve suojella asianosaisen yksityisyyttä huoltajilta. Näiden säännösten osalta on kuitenkin syytä huomioida, että sähköisen asioinnin mahdollistaminen ei todennäköisesti edesauta alaikäisen asianosaisen itsenäistä asiointia, koska ei ole olemassa mitään keinoa varmistua siitä, käyttääkö välinettä alaikäinen itse vai hänen huoltajansa.

Lain digitaalisesta henkilöllisyystodistuksesta 11 § 3 momentin osalta on lisäksi todettava, että digitaalisen henkilöllisyystodistuksen haltijan vastuu on kirjattu ristiriitaisesti säännökseen ja sen perusteluihin. Säännöksessä todetaan, että katoamisesta on ilmoitettava ilman aiheetonta viivytystä DVV:lle. Säännöksessä ei ole millään tavalla otettu kantaa ilmoituksen oikeusvaikutuksiin suhteessa käyttäjän vastuuseen. Kyseisen säännöksen yksityiskohtaisissa perusteluissa on kuitenkin todettu seuraavasti *Ilmoitus olisi tehtävä Digi- ja väestötietovirastolle ilman aiheetonta viivytystä sen jälkeen, kun digitaalisen henkilöllisyystodistuksen haltija on havainnut asian. Digitaalisen henkilöllisyystodistuksen vastuu todistuksen oikeudettomasta käytöstä päättyisi sen jälkeen, kun ilmoitus on tehty.*

Poliisihallitus pitää ehdottoman kannatettavana sitä, että käyttäjään kohdistuu ankara vastuu oikeustoimista, jotka välineellä on tehty, jos ilmoitusta katoamisesta ei ole tehty ajoissa. Säännös tulisi vastata sisällöllisesti tunnistuslain 27 §:ää, jossa on säännelty tunnistusvälineen haltijan tunnistusvälineen oikeudetonta käyttöä koskevat vastuunrajoitukset. Ankara vastuu on käytännössä ainoa asia, joka estää ihmisiä luovuttamasta tunnistusvälinettä vilpillisessä mielin käytettäväksi rikollisiin tarkoituksiin. Jos välineen haltijaan ei kohdistu ankara vastuu, voisi tilanne mennä esimerkiksi seuraavasti: henkilö A luovuttaa välineensä henkilön B haltuun tarkoituksena, että henkilö B tekee petosrikoksen käyttäen välinettä hyväksi. Henkilö A kertoo, että väline ei ole ollut hänen hallussa. Jos ilmoituksen tekemättä jättämiseen ei sovelleta ankaraa vastuuta, tulee kuvattua menettelyä hyödyntävät petokset lisääntymään olennaisesti.

## Digitaalisen henkilöllisyystodistuksen peruuttaminen ja tietojen ajantasaisuus

Ehdotuksessa laiksi digitaalisesta henkilöllisyystodistuksesta 8 §:ssä määritellään edellytykset kyseisen välineen peruuttamiselle. Peruuttamisedellytyksiä koskeva sääntely on poliisin näkökulmasta sisällöllisesti tarkoituksenmukainen, mutta peruuttamisen seurauksista olisi syytä säännellä täsmällisemmin. Sääntelyssä tai vähintään säännöksen perusteluissa tulisi korostaa sitä, että välineen käytön on estyttävä välittömästi, kun peruutusta koskeva päätös on tehty.

Esimerkiksi tilanteessa, jossa henkilö on onnistunut erehdyttämään viranomaisia siten, että hän on onnistunut saamaan digitaalisen henkilöllisyystodistuksen väärillä tiedoilla, on ehdottoman tärkeää, ettei välineen käyttäminen ole mahdollista enää siinä vaiheessa, kun väärin perustein saatu passi tai henkilökortti on peruutettu. Toinen vastaava tilanne, jossa välineen käytön välitön estäminen on tärkeää, on silloin, jos passi tai henkilökortti on viranomaisen tekemän virheen takia myönnetty väärillä tiedoilla.

Sääntelyn ongelmallisuutta tämän asian suhteen lisää se, että 10 § 2 momentissa on tarkoitus säännellä digitaalisen henkilöllisyystodistuksen käyttämisestä käyntiasioinnissa siten, että ydinidentiteetin todisteen voimassaolon varmentaminen on vapaaehtoista. Mikäli ajantasaisuuden varmentaminen on vapaaehtoista, olisi peruutettujen digitaalisten henkilöllisyystodistusten käytön estämiseksi rakennettava jonkinlainen toissijainen esimerkiksi sulkulistan tapainen järjestely, joka on jokaisen tapahtuman yhteydessä tarkastettava. Muussa tapauksessa tämä tiedon ajantasaisuuteen liittyvä pulma vaarantaa luottamuksen digitaaliseen henkilöllisyystodistukseen ja yleisemmin viranomaisten välittämään tietoon. Lisäksi Poliisihallitus korostaa sitä, että hankkeen tavoitteena on ollut luoda väline, joka välittää nimenomaa ajantasaista tietoa henkilöllisyydestä.

Turvallisempi ratkaisu olisi kuitenkin se, että tietojen ajantasaisuus tarkastettaisiin lähtökohtaisesti aina. Tästä peruslähtökohdasta olisi tarkoituksenmukaista voida poiketa ainoastaan tarkasti rajattujen edellytysten täyttyessä. Kun sääntelyssä on omaksuttu toimintamalli, jossa tietojen ajantasaisuuden tarkistaminen on vapaaehtoista, tarkoittaa se monesti käytännön tasolla sitä, ettei ajantasaisuutta tarkisteta kuin äärimmäisen harvoin, mitä ei voida pitää tarkoituksenmukaisena asiaintilana.

Tiedon ajantasaisuuden tasoa ja sen tarkastamista koskien lienee perusteltua käsitellä hallituksen esityksen jatkovalmistelussa myös kysymystä vastuusta suhteessa digitaalisen henkilöllisyystodistuksen sisältämään vanhentuneeseen tai väärään tietoon. Missä tilanteissa viranomainen on vahingonkorvausvastuussa, jos tarkastaja on luottanut digitaalisen henkilöllisyystodistuksen tietoihin, jotka osoittautuvat vääriksi. Viranomaisen vastuu tullee kysymykseen ainakin niissä tilanteissa, joissa viranomaisen tiedossa on ollut välineen väärä tietosisältö, mutta sen käyttöä on voitu jatkaa eikä sitä ole voitu välittömästi peruuttaa esim. sulkulistan avulla. Toinen kysymys on sitten se voiko vastuu jäädä tarkastajalle tilanteissa, joissa hän ei ole tarkistanut digitaalisen henkilöllisyystodistuksen ajantasaisuutta. Tätä lähtökohtaa on kuitenkin vaikea pitää perusteltuna siitä näkökulmasta, että luonnoksessa hallituksen esitykseksi tarkastaminen on tietoisesti jätetty harkinnanvaraiseksi.

Poliisihallituksen näkemyksen mukaan toiminnan turvallisuuden ja digitaalisen henkilöllisyyden hankkeelle asetettujen tavoitteiden saavuttamisen näkökulmasta perustellumpaa olisi, että digitaalisen henkilöllisyystodistuksen tietojen ajantasaisuus tarkistetaan aina käyntiasioinnin yhteydessä tai vähintään estetään peruutettujen välineiden käyttäminen pakollisen sulkulistatarkastamisen kautta.

## Päätöksenteko peruutustilanteessa

Lain digitaalisesta henkilöllisyystodistuksesta 8 §:ssä on tarkoitus säännellä peruuttamisedellytyksistä. Peruutusedellytykset ovat Poliisihallituksen näkökulmasta pääasiallisesti riittävät. Sääntelyyn voisi tarkoituksenmukaisuuden vuoksi lisätä kuitenkin säännöksen siitä, mitä tapahtuu tilanteessa, jossa välineen haltija menehtyy. Peruutetaanko väline vai tapahtuuko jonkinasteinen raukeaminen.

Peruuttamisedellytysten osalta säännellään ehdotuksessa tällä hetkellä siten, että digitaalinen henkilöllisyys perutaan pykälän 1 momentin mukaan ilman harkintaa ja aina tilanteissa, joissa sen haltija pyytää peruuttamista tai laite, jossa digitaalinen henkilöllisyystodistuksen sisältämä laite on ilmoitettu kadonneeksi tai anastetuksi. 2 momentissa mainituissa tilanteissa on kyse peruuttamisperusteista, jotka kuuluvat poliisin toimivaltaan.

Sääntely ei ota kantaa 8 § 1 momentin osalta siihen, kenen tehtävä peruuttaminen tällaisissa tilanteissa on. Toteutuksessa on suunniteltu, että tällaisissa tapauksissa välineen haltija olisi ensisijaisesti yhteydessä DVV:hen, joka huolehtii välineen peruuttamisesta peruuttamalla ydinidentiteetin varmenteen. Toisaalta lienee mahdollista, että asia tulee esiin asioitaessa poliisin luona, jolloin olisi perusteltua, että myös poliisi voisi peruuttaa välineen. Selkeyden vuoksi voisikin olla perusteltua säännellä täsmällisemmin viranomaisten välisestä tehtävänjaosta 8 § 1 momentin tarkoittamissa tilanteissa.

Toinen peruuttamisiin liittyvä seikka, joka kaipaa täsmentämistä on päätöksenteko. Hallituksen esityksen luonnos ei ota kantaa siihen tehdäänkö peruuttamisen osalta erillinen hallintopäätös. Hallintoprosessin peruslähtökohtana on se, että kaikista myöntämistä tai peruuttamista koskevista asiaoista tehdään päätös, jos tästä perusolettamasta halutaan poiketa, olisi siitä säänneltävä selkeästi, kuten on tehty digitaalisen henkilöllisyystodistuksen myöntämisen osalta. Ehdotetun sääntelyn muotoilu tarkoittaisi käytännössä sitä, että kaikista peruuttamista koskevista toimenpiteistä tulisi tehdä erillinen päätös.

Ottaen huomioon digitaalisen henkilöllisyystodistuksen erityispiirteet, johdonmukaisinta olisi, että kaikista peruuttamista koskevista toimenpiteistä ei tehtäisi erillistä tiedoksi annettavaa hallintopäätöstä, johon voidaan hakea muutosta. Välineissä tapahtuu jatkuvasti muutoksia, kun laitteita hukataan, ne rikkoutuvat tai muuten vaan uusitaan. Digitaalinen henkilöllisyystodistus on helppo ottaa uudestaan käyttöön samoin edellytyksin kuin aiemmin.

Käytännössä digitaalisen henkilöllisyystodistuksen peruuttamista koskeva toimenpide ei suoranaisesti vaikuta henkilön oikeusasemaan. Henkilön oikeus käyttää ja ottaa uudelleen käyttöön digitaalinen henkilöllisyystodistus on riippuvainen puhtaasti passin tai henkilökortin olemassaolosta eikä erillisestä viranomaisen päätöksestä. Viranomaisilla ei ole käytännössä mahdollisuutta estää tiettyä henkilöä ottamasta välinettä välittömästi uudelleen käyttöön peruuttamisen jälkeen.

Välineen uudelleen käyttöönottaminen estyy ainoastaan tilanteessa, jossa digitaalisen henkilöllisyystodistuksen perusteena oleva passi tai henkilökortti peruutetaan eikä henkilöllä ole toista henkilöllisyysasiakirjaa. Tällaisessa tilanteessa hän menettää oikeuden digitaalisen henkilöllisyystodistuksen käyttöön. Tällaisessakaan tilanteessa ei ole kuitenkaan tarpeellista tehdä asiasta erillistä päätöstä, koska toimenpide seuraa suoraan passia tai henkilökorttia koskevasta päätöksestä. Oikeus digitaaliseen henkilöllisyystodistukseen ei ole asia, josta viranomainen voisi erikseen päättää, vaan se on ehdotetun sääntelyn mukaan suora seuraus passin tai henkilökortin voimassaolosta.

Poliisihallituksen näkemyksen mukaan sääntelyä tulisikin siis täsmentää siten, ettei digitaalisen henkilöllisyystodistuksen peruuttamista koskevasta toimenpiteestä tehdä erillistä hallintopäätöstä. Tämä saattaa myös edellyttää sitä, että 8 § 2 momentin peruuttamisedellytyksiä täsmennetään siten, ettei niihin sisälly harkinnanvaraa, kuten tämänhetkisessä luonnoksessa hallituksen esitykseksi.

## Käyntiasioinnin siirtymäsäännös

Digitaalisen henkilöllisyystodistuksen käyntiasiointiin tarkoitettuja toimintoja koskevaan sääntelyyn liittyy siirtymäsäännös koskien DVV:n määräystä koskien muiden tahojen mahdollisuutta tuottaa henkilöllisyystodistuksen tarkastustoiminnallisuus. Alkuvaiheessa käytössä olisi ainoastaan DVV:n laatima mobiililaitteessa toimiva tarkastussovellus. Käytännössä tämä tarkoittaa sitä, että alkuvaiheessa kaupan tai minkään muunkaan alan toimijat eivät voi integroida digitaalisen henkilöllisyystodistuksen tarkastamista osaksi omia tietojärjestelmiään, vaan tarkastus on tehtävä erillisellä mobiililaitteella.

Tällaisessa toimintamallissa henkilöllisyyden tarkastaminen vertautuu tarkastajan näkökulmasta hyvin pitkälti perinteisiin tunnistusratkaisuihin siinä mielessä, että se ei tarjoa mitään lisää. Tiedot on tarkistettava mobiililaitteen näytöltä eikä niitä voida suoraan siirtää käsittelyjärjestelmään. Toimijoiden omien tarkastussovellusten käyttöönotto mahdollistaa esimerkiksi sen, että tiedot asioivasta henkilöstä siirretään automaattisesti järjestelmään. Tämä nopeuttaa huomattavasti asiointia tilanteissa, joissa järjestelmään on tehtävä kirjaus henkilöstö, joka on asioinut tai esimerkiksi perustettaessa asiakassuhdetta.

Poliisihallitus esittää huolensa liittyen käyntiasioinnin järjestämiseen. Digitaalisen henkilöllisyystodistuksen suosio ja käytettävyys määrittyvät hyvin pitkälti sen mukaan, missä asioinnissa välinettä on mahdollista käyttää. Mitä harvemmassa asiointipaikassa sen tarkastamiseen on mahdollisuus, sitä harvempi ihminen ottaa välineen käyttöön. Toisaalta, jos vain harva ottaa välineen käyttöön, ei monella yksityisen sektorin toimijalla ole varsinaista intressiä mahdollistaa välineen käyttöä varsinkaan, jos välineestä ei saada mitään etua suhteessa perinteiseen tunnistamistapaan.

Kattavasti digitaalisen henkilöllisyystodistuksen hyväksymiseen velvoittavaa sääntelyä on vaikea istuttaa Suomen oikeusjärjestelmään, koska vastaavaa ei ole edes perinteisten passin ja henkilökortin osalta. On mahdollista säännellä yksittäisistä käyttötapauksista, kuten hallituksen esityksen luonnoksessa onkin tehty tunnistuslain ensitunnistamista koskevan sääntelyn osalta. Laajan käyttöasteen saavuttamiseksi avainasemassa on se, että digitaalisen henkilöllisyystodistuksen käyttöönottaminen henkilöllisyyden tai iän osoittamiseen on eri toimialoille houkuttelevaa. Tästä syystä olisi tärkeää, että erilaisia digitaalisen henkilöllisyystodistuksen hyödyntämiseen tarvittavia tarkastussovelluksia on mahdollista ottaa käyttöön mahdollisimman pian välineen käyttöönoton jälkeen. Ideaalissa tilanteessa tarkastusmahdollisuudet olisivat olemassa jo itse välineen julkaisuajankohtana.

# Ulkomaalaisen asiointiväline

Ulkomaalaisen asiointiväline on DVV:n toimivaltaan kuuluva väline, jonka tuottamiseen poliisi ei osallistu. Poliisihallituksen lausunto keskittyy siten puhtaasti muutoksen vaikutuksiin yhteiskunnassa ja sen mahdolliseen vaikutuksiin rikollisen toiminnan näkökulmasta. Ehdotettu ulkomaalaisen asiointiväline nivoutuu hyvin vahvasti yhteen henkilötunnuksen uudistamista koskevan lakimuutoksen kanssa. Yhdessä muutosten seurauksena on tarkoitus mahdollistaa ulkomaalaisen henkilön rekisteröityminen etämenettelyn avulla Väestötietojärjestelmään ja myöntää sähköisen asioinnin mahdollistava väline. VTJ-rekisteröitymisen yhteydessä henkilölle luodaan henkilötunnus.

Poliisihallituksen asiantuntijat ovat antaneet tukea määriteltäessä etärekisteröintimenettelylle asetettavia edellytyksiä, jotta menettely saadaan niin turvalliselle tasolle kuin se on etänä mahdollista. Etärekisteröintiin kuitenkin liittyy omat ilmeiset rajoitteensa, jotka ovat syytä saada iskostettua laajasti kaikkeen yhteiskunnalliseen toimintaan, jotta laajamittaisilta väärinkäytöspyrkimyksiltä vältytään. Käytännössä etämenettelyn avulla voidaan luotettavasti saada selville, että matkustusasiakirjaan merkittyjen henkilötietojen joukko muodostaa kokonaisuuden eli tällainen henkilö on olemassa ja hänelle on myönnetty kyseisen maan passi. Menettelyn avulla ei ole kuitenkaan täysin luotettavalla tavalla mahdollista varmistua siitä, että rekisterihenkilöllisyyden saa haltuunsa kyseinen henkilö.

Lyhyesti todettuna etärekisteröinnin on määrä tapahtua seuraavasti:

- henkilö lataa sovelluksen mobiilipäätelaitteelleen
- Sovellus lukee passin sirun ja sirun tietojen alkuperä ja muuttumattomuus varmistetaan
- hänen etäyhteydellä välittyviä kasvojaan verrataan sirulta luettuun kuvaan
- tämän jälkeen henkilö rekisteröidään automaattisesti VTJ:hin

Suunniteltu etärekisteröintimenettely mahdollistaa sen, että rekisteröinti voidaan pyrkiä tekemään toiselle henkilölle kuuluvan kadonneen tai anastetun matkustusasiakirjan avulla. Toinen potentiaalinen väärinkäytöksen tapa voi olla esimerkiksi se, että vaihtamalla nimeä tai käyttämällä toisen maan myöntämää passia pyritään saamaan käyttöön useita henkilöllisyyksiä Suomeen. Erilaisten väärinkäytösyritysten houkuttelevuutta lisää nykyiseen tilanteeseen verrattuna erityisesti se, että kaikki tapahtuu etänä ja kiinnijäämisen riski on erittäin pieni, vaikka henkilö pyrkisi toistuvasti rekisteröitymään eri henkilöille kuuluvilla matkustusasiakirjoilla. Rekisterimerkintärikoksen tekopaikasta huolimatta rikollinen toiminta suuntautuisi Suomeen. Näin toteutettujen rikosten esitutkinta on erittäin hankalaa, sillä ulkomailla oleskeleva rikoksesta epäilty ei ole helposti tavoitettavissa esitutkintaan Suomessa.

Etäyhteyden välityksellä tapahtuvan rekisteröinnin Akilleen kantapää on kasvojentunnistaminen, johon liittyy olennaisia riskitekijöitä, koska tila ja laite, jolla tunnistus suoritetaan, ovat täysin rekisteröityvän henkilön itsensä hallinnassa. Kasvontunnistusohjelmia on pystytty huijaamaan erilaisilla fyysisillä ja digitaalisilla maskeilla ja muilla keinoin. Etärekisteröintimenettelyssä on mahdollista hyödyntää erilaisten jopa yleisesti verkossa saatavien sovellusten avulla tapahtuvaa manipulaatiota, jonka avulla saadaan videolla todellisuudessa esiintyvä henkilö näyttämään aivan toiselta henkilöltä (deepfake). Manipulaatio voidaan saada tehtyä esim. matkustusasiakirjassa olevan kuvan pohjalta. Rekisteröinti voidaan pyrkiä tekemään toiselle henkilölle kuuluvan kadonneen tai anastetun matkustusasiakirjan avulla.

Tarkemmin sanottuna menettely ei ainoastaan mahdollista väärinkäytösyrityksiä vaan jo tässä vaiheessa on täysin varmaa, että sitä pyritään ja todennäköisesti onnistutaan käyttämään väärin. Useiden identiteettien hankintaa voidaan yrittää hyödyntää myöhemmin erilaisten petosten tehtailuun. Etärekisteröinnin käyttöönotossa olennaisinta onkin se, että kaikille yhteiskunnan toimijoille on selkeää, ettei etärekisteröityyn henkilöllisyyteen ja sen perusteella saatuun ulkomaalaisen asiointivälineeseen tule luottaa samalla tavoin kuin perinteiseen tapaan rekisteröityihin henkilöllisyyksiin ja niiden perusteella saatuihin tunnistusvälineisiin.

Lainsäädännön tasolta asiaa tarkasteltaessa ei etärekisteröinnin pitäisi aiheuttaa merkittäviä ongelmia, koska pelkkä henkilötunnuksen saaminen ei luo mitään oikeuksia eikä ulkomaalaisen asiointiväline itsessään luo kuvaa siitä, että taustalla oleva henkilöllisyys kuuluisi todella sille henkilölle, joka välinettä käyttää. Käytännössä kuitenkin tilanne voi olla toinen ja etärekisteröidyn henkilöllisyyden sisältävää ulkomaalaisen asiointivälinettä voidaan pyrkiä käyttämään erehdyttämiseen etenkin yksityisten henkilöiden välisessä kanssakäymisessä sekä sellaisessa yritystoiminnassa, jossa henkilötietoja ei tarkisteta suoraan väestötietojärjestelmästä.

Poliisihallitus on lisäksi tuonut esille sen, että etärekisteröintimenetelmää voisi olla mahdollista hyödyntää myös haittaamistarkoituksessa tekemällä organisoidusti isoja määriä etärekisteröintejä tuottaen näin väestötietojärjestelmään lukuisia uusia rekisteröityjä ja näin vaikuttaen perusrekisterin toimintaan ja tietosisällön yleiseen luotettavuuteen. Poliisitoiminnassa on lisäksi tunnistettu merkittävä määrä tapauksia, joissa rekisterimerkintöjen luomiseen on käytetty tietoja henkilöistä, jotka ovat tietoisia heidän tiedoillaan tehtävien rekisterimerkintöjen päätymisestä rikollisiin tarkoituksiin. Näissä tapauksissa rekisterimerkintöjen tekeminen on voitu suorittaa rahallista korvausta vastaan.

Käytännössä on lähes mahdotonta ennakolta arvioida, kuinka paljon erityyppiset rikokset tulevat lisääntymään etärekisteröinnin perusteella. Tähän vaikuttaa erityisesti se, miten uusi menettely ja siihen liittyvät mahdolliset riskit tullaan sisäistämään yhteiskunnassa. Muutos nykyiseen tilaan verrattuna on hyvin suuri ja riskinä on, että ihmisten epätietoisuutta muutoksesta pyritään käyttämään hyväksi rikollisiin tarkoituksiin. Mikäli etärekisteröidyn henkilöllisyyden sisältävän ulkomaalaisen asiointivälineen käytettävyyttä ei rajoiteta koskemaan vain tiettyjä rajattuja toimijoita, riskinä on, että yhteisvaikutuksena luodaan tehokkaat välineet rikollisten hyödynnettäväksi.

# Kommentit ydinidentiteetin todisteesta

Ydinidentiteetin todiste on Digi- ja väestötietoviraston tuottama todistetta, jonka avulla voidaan luotettavasti osoittaa, että todisteen haltija on ydinidentiteetin yksilöimä henkilö. Ydinidentiteetin todiste sisältyy niin digitaaliseen henkilöllisyystodistukseen kuin ulkomaalaisen asiointivälineeseenkin.

## Ydinidentiteetin voimassaoloaika

Ehdotuksessa laiksi Digi- ja väestötietoviraston digitaalisen henkilöllisyyden palveluista 12 §:n mukaan [1 mom.] Ydinidentiteetin todisteen voimassaolo päättyy vuoden kuluttua siitä, kun ydinidentiteetin todisteen rekisteröinnin perustana olleen henkilöllisyyttä osoittavan asiakirjan voimassaolo on päättynyt. [2 mom.] Henkilöllisyyttä osoittavalla asiakirjalla tarkoitetaan digitaalisen henkilöllisyystodistuksen osalta sitä passilain tai henkilökorttilain mukaisesti myönnettyä henkilöllisyyttä osoittavaa asiakirjaa, jonka perusteella digitaalinen henkilöllisyystodistus on otettu käyttöön.

Vastaavalla tavalla kuin yllä on esitetty digitaalisen henkilöllisyystodistuksen käyttöönoton yhteydessä määriteltävän tietosisällön osalta myös voimassaoloaika olisi perusteltua määrittyä tuoreimman henkilöllisyysasiakirjan perusteella eikä sillä perusteella, mitä asiakirjaa henkilö on esittänyt käyttöönoton yhteydessä.

Esimerkiksi tilanteessa, jossa henkilön passi on voimassa neljä vuotta ja henkilökortti, jolla hän ottaa välineen käyttöön on voimassa kaksi vuotta, olisi perusteltua, että voimassaoloaika määräytyy pisimpään voimassaolevan henkilöllisyysasiakirjan perusteella. Käyttöönoton yhteydessä esitettävän passin tai henkilökortin tarkoitus on ensisijaisesti vahvistaa sähköisesti tapahtuvan tunnistamistilanteen luotettavuutta eikä toimia digitaalisen henkilöllisyystodistuksen tietojen lähteenä. Tiedot siirtyvät käyttöönotettavaan digitaalisen henkilöllisyystodistuksen suoraan rekisteristä ja siksi olisi perusteltua, että käytetään sitä digitaaliseen henkilöllisyystodistukseen oikeuttavaa henkilöllisyysasiakirjaa, jossa on ajantasaiset tiedot ja pisin voimassaoloaika.

## Ydinidentiteetin elinkaari

Luonnos hallituksen esitykseksi jättää auki olennaisen kysymyksen ydinidentiteetin todisteen ja siten myös digitaalisen henkilöllisyystodistuksen elinkaaresta. Molemmille on määritelty käyttöönotosta laskettava voimassaoloaika, mutta kysymys siitä mitä ydinidentiteetin todisteille muissa tilanteissa tapahtuu jää auki.

Määrittelemättömän tilan keskeisin ongelma nousee esiin tilanteessa, jossa henkilölle myönnetään uusi passi tai henkilökortti ja hän haluaa päivittää mahdollisesti muuttuneet henkilötiedot, mutta ennen kaikkea voimassaoloajan myös digitaaliseen henkilöllisyystodistukseen. Syntyykö tällaisessa tilanteessa uusi ydinidentiteetin todiste vai jatkuuko aiemman voimassaoloaika ja mikä merkitys sillä on, jos esimerkiksi nimi on vaihtunut. Vastaavasti kysymys ydinidentiteetin elinkaaresta on esillä tilanteissa, joissa käyttäjä hankkii uuden mobiililaitteen, jossa hän haluaa siirtää jo käytössään olevan digitaalisen henkilöllisyystodistuksen.

Sinänsä valittavalla sääntelytavalla ei ole poliisin toiminnan näkökulmasta suurta merkitystä, mutta olisi olennaista, että asiaa koskeva sääntely lisätään hallituksen esityksen jatkovalmistelussa.

## Ydinidentiteetin osoittamat tiedot

Digi- ja väestötietoviraston digitaalisen henkilöllisyyden palveluista annetun lain 10 §:ssä esitetään säädettäväksi ydinidentiteetin todisteesta, joka sisältyisi niin digitaaliseen henkilöllisyystodistukseen kuin ulkomaalaisen henkilön asiointivälineeseen. Säädöksessä todetaan, että ydinidentiteetin todisteella tarkoitettaisiin sellaista Digi- ja väestötietoviraston tuottamaa todistetta, jonka avulla voidaan luotettavasti osoittaa, että todisteen haltija on ydinidentiteetin yksilöimä henkilö.

Tämän lausunnon ulkomaalaisen asiointivälinettä ja etärekisteröityä identiteettiä käsittelevässä kohdassa on tuotu esille seikkoja, joiden vuoksi etärekisteröintimenettelyllä ei voida luotettavalla tavalla varmistua rekisteröityvän henkilön henkilöllisyydestä. Menettelyssä voitaneen kohtuullisen luotettavasti varmistua kyseisen passin olemassaolosta sekä siitä, kenelle passi on myönnetty. Toisaalta on syytä muistaa, ettei menettelyn avulla saada riittävää varmuutta siitä, kuuluuko esitetty passi henkilölle, joka on sitä esittänyt ja joka siis saa käyttöönsä ulkomaalaisen asiointivälineen. Tästä syystä on hyvä huomata, ettei 10 §:n 1 momentin mukaisesti ydinidentiteetin todisteella voida kaikissa tilanteissa osoittaa luotettavalla tavalla sitä, että sen haltija olisi ydinidentiteetin osoittama henkilö.

# Luonnollisen henkilön tunnistusväline

Luonnollisen henkilön tunnistusväline tai niin sanottu vaihtoehtoinen väline on DVV:n toimivaltaan kuuluva kokonaisuus. Ratkaisun tarkoituksena on ollut tarjota vaihtoehtoinen tapa toteuttaa digitaalinen henkilöllisyystodistus sellaisten henkilöiden osalta, jotka eivät käytä mobiililaitetta ja siten hyödynnä digitaalista henkilöllisyystodistusta. Käytännössä sääntelyn perusteella toteutettava väline olisi viranomaisten sähköisten palvelujen käyttämisen mahdollista väline, joka voimassaolevan passin tai henkilökortin haltijan olisi mahdollista saada digitaalisen henkilöllisyystodistuksen sijaan Luonnollisen henkilön asiointivälineeseen liittyy useita avoimia kysymyksiä niin sen saamisen kuin siitä aiheutuvien kustannusten osalta, joita jatkovalmistelussa on syytä pohtia. Arvioitaessa ratkaisua tulisi pyrkiä mahdollisimman kustannustehokkaaseen vaihtoehtoon, jotta menekiltään vähäisen välineen kustannukset eivät vaikuta kohtuuttomasti passien ja henkilökorttien suoritemaksuihin, joihin vaihtoehtoisesta välineestä syntyvät kustannukset on määrä vyöryttää.

# Laki henkilötietojen käsittelystä poliisitoimessa annetun lain muuttamisesta

Poliisin henkilötietolakiin esitetään muutoksia poliisin tiedonsaantioikeuksiin (16 §) ja muuhun tietojen luovuttamiseen viranomaisille (22 §).

Lain 16 pykälän 1 momenttia ehdotetaan muutettavaksi siten, että siihen lisättäisiin uusi 16 kohta, jonka perusteella poliisilla olisi oikeus saada tietoja Digi- ja väestötietoviraston digitaalisen henkilöllisyyden palveluista annetun lain mukaisesti ydinidentiteetin todisteen myöntämiseksi sekä digitaalisen henkilöllisyystodistuksen tuottamiseksi välttämättömistä tiedoista. Koska digitaalisen henkilöllisyystodistuksen käyttöönotto voi potentiaalisesti lisätä riskiä väärinkäytöksiin, poliisin henkilötietolain 16 §:n päivittämisen osalta tietojensaantioikeuden DVVltä tulisi koskea myös edellä todettujen tietojen saamiseksi poliisille henkilötietojen väärinkäyttöepäilyjen, identiteettivarkauksien tai muiden vastaavien rikosten selvittämiseksi ja näiden ennalta estämiseksi.

Lain 22 pykälän 1 momenttia ehdotetaan esityksessä muutettavaksi siten, että siihen lisättäisiin uusi 18 kohta, jonka perusteella poliisi saisi salassapitosäännösten estämättä luovuttaa teknisen käyttöyhteyden avulla tai tietojoukkona 5-8, 11 ja 12 §:ssä tarkoitettuja henkilötietoja viranomaisen laissa säädetyn tehtävän suorittamiseksi Digi- ja väestötietovirastolle Digi- ja väestötietoviraston digitaalisen henkilöllisyyden palveluista annetussa laissa tarkoitettujen digitaalisen henkilöllisyyden tietojärjestelmän ja ydinidentiteetin tuottamista ja hallinnointia varten. Muotoilu on väljä. Esikunnan näkemyksen mukaan tietojen luovuttamisen Digi- ja väestötietovirastolle tulisi täsmentää ja rajautua niihin poliisin henkilötietolain 11-12 §:n tietoihin, jotka ovat välttämättömiä digitaalisen henkilöllisyyden tietojärjestelmän ja ydinidentiteetin tuottamista ja hallinnointia varten. Esityksen pohjalta arvioituna esikunnassa ei ole tunnistettu, miten poliisin henkilötietolain 5-8 §:n mukaiset tiedot olisivat tai voisivat olla välttämättömiä DVVn tehtävän suorittamiseksi.

Lisäksi esitetään arvioitavaksi, onko poliisin henkilötietolain 4 §:ää ja 12 §:ää tarpeen päivittää käsiteltävien tietojen osalta vai ovatko em. pykälissä yksilöidyt tiedot riittävät

# Tunnistuslaki

Lakia vahvasta sähköisestä tunnistamisesta ja sähköisistä luottamuspalveluista ehdotetaan muutettavan muun muassa siten, että 7 b §:ssä määritellyn poliisin tarjoaman niin sanotun voimassaolopalvelun käytöstä tehtäisiin pakollista, kun ensitunnistaminen tehdään Suomen viranomaisen myöntämän passin tai henkilökortin perusteella. Muutoksen tavoitteena on lisätä monta vuotta käytössä olleen palvelun valitettavan pienelle tasolle jäänyttä käyttöastetta. Nykyisellään suurin osa tunnistuspalvelujen tarjoajista ei käytä palvelua lainkaan.

Poliisihallitus pitää ehdotettua muutosta lähtökohtaisesti erittäin kannatettavana. Poliisihallitus kuitenkin tunnistaa muodoltaan ehdottomaan sääntelyyn liittyvän riskin tilanteessa, jossa tietoliikenneyhteyksissä on syystä tai toisesta sellaista häiriötä, joka estää voimassaolon tarkistamisen. Tällaisessa tilanteessa asiointitilanne keskeytyy. Erityisen ongelmalliseksi keskeytymisen tekee se, että se koskee vain ja ainoastaan sellaisia henkilöitä, joiden ensitunnistamiseen käytetään Suomen viranomaisen myöntämiä passia tai henkilökorttia. Ulkomaalaisen henkilöllisyysasiakirjan osalta ensitunnistaminen ei estyisi, koska poliisin voimassaolopalvelua voidaan hyödyntää ainoastaan Suomen passeihin ja henkilökortteihin.

Sääntelyssä tai sen perusteluissa voisi olla selventävää todeta, että tietoliikenteessä olevan häiriön aikana voisi ensitunnistamiseen liittyvän voimassaolotarkastuksen tehdä jälkikäteisesti. Tällaisen poikkeaman tekeminen ei olennaisesti heikentäisi esitetyn muutoksen turvallisuustoimenpiteen tehokkuutta eikä suomalaisen henkilöllisyystodistuksen haltija asettuisi heikompaan asemaan suhteessa muun maan passin tai henkilökortin haltijaan.

# Tietosuojaa ja digitaalisesta henkilöllisyystodistuksesta annettavaa lakia koskevan huomiot

Poliisihallituksen esikunta on tuonut esille selkeän tarpeen arvioida tietosuojan näkökulmasta digitaalisten henkilöllisyystodistuksen myöntämiseen ja tietojen välittämiseen Digi- ja väestötietovirastolle kaavaillun teknisen ratkaisun. Toteutus on suunniteltu siten, että Turvaverkon ulkopuolelle eTuven ympäristöön sijoittuvaan edustapalveluun olisi tarkoitus tuoda kaikkien passi- ja henkilökorttirekisteriin talletettujen henkilöiden tiedot, joilla on voimassa olevia dokumentteja. Tiedot tuotaisiin tietosisällöltään osin rajatusti, jolloin ne eivät mm. sisällä sormenjälkitietoja tai lupa-asiakirjojen asiakirjanumeroita.

Hallituksen esityksen perusteluissa on todettuna tästä teknisestä toteutustavasta, mutta ei sen kattavuudesta myös niihin henkilöihin, jotka eivät ole ottaneet käyttöönsä digitaalista henkilöllisyystodistusta. Esikunta nostaa esille sen, että passi- ja henkilökorttirekisterin tietojen käsittelyssä tähän tarkoitukseen tulisi säännellä selkeästi. Sääntelyssä olisi nostettava esille mahdollisuus käsitellä kaikkien voimassaolevien henkilökorttien ja passien digitaalisesta henkilöllisyydestä esitetyn lain 5§:n mukaisia tietoja.

Digitaalisesta henkilöllisyystodistuksista esitetyn lain 4 §:ssä säädettäisiin rekisteristä digitaalisista henkilöllisyystodistuksista. Poliisi toimisi kyseisen rekisterin rekisterinpitäjänä ja sen tehtävänä olisi ylläpitää rekisteriä digitaalisista henkilöllisyystodistuksista, niiden haltijoista ja todistusten voimassaolosta. Rekisterin käyttötarkoitus olisi digitaalisten henkilöllisyystodistusten tarjoaminen ja tuottaminen. Edellä mainitun 4 §:n sisältö on varsin suppea, eikä se sisällä esimerkiksi viittausta poliisin henkilötietolakiin (Laki henkilötietojen käsittelystä poliisitoimessa, 616/2019), jossa säädettyä sovellettaneen digitaalisesta henkilöllisyystodistuksesta esitetyn lain perusteella käsiteltäviin henkilötietoihin.

Esitetyn lain 4 §:n sijaan henkilötietojen käsittelystä todetaan ainoastaan pykäläkohtaisissa perusteluissa ja digitaalisen henkilöllisyystodistuksen haltijalle toimitettavasta sisällöstä esitysluonnoksen 5 §:ssä. Kyseisessä, poliisin rekisteriä koskevassa 4 pykälässä olisi tarpeen todeta käsiteltävien tietojen sisältö. Lisäksi pykälätekstiin olisi tarpeen yksilöity tieto siitä, että kyseisessä rekisterissä käsiteltävien tietojen käytöstä, luovuttamisesta ja poistamisesta säädetään poliisin henkilötietolaissa (laki henkilötietojen käsittelystä poliisitoimessa) annetussa laissa.

Esitysluonnoksen 5 §:ssä on yksilöity tiedot, jotka poliisi toimittaisi digitaalisen henkilöllisyystodistuksen haltijalle. Kyseisen 5 §:n 3 momentin mukaan Digitaalisen henkilöllisyystodistuksen käytön edellytyksenä on, että sen sisältämät tiedot ovat aina ajan tasalla ja vastaavat poliisin 1 momentin rekistereissä olevia tietoja. Vaatimus johtuu tietosuojalainsäädännön tietojen oikeellisuus- ja ajantasaisuusvaatimuksesta ja edellyttää sitä, että passi- ja henkilökorttirekisterin tiedot on pidettävä ajan tasalla ja näiden tietojen ajantasaisuus olisi virkistettävä taajaan digitaalisten henkilöllisyystodistusten rekisteriin. Esityksessä voisi olla aiheellista todeta siitä, kuinka pitkä viive päivityksessä voitaisiin katsoa mahdolliseksi.

## Tietojen käsittely ja tiedon elinkaaren hallinta

Tiedon elinkaaren hallinnan näkökulmasta tuodaan esille seuraavaa: Hallituksen esitysluonnoksen 4 §:ssä on esitetty säädettäväksi, että poliisi ylläpitää rekisteriä myönnetyistä digitaalisista henkilöllisyystodistuksista. Tässä yhteydessä tulisi säätää myös tietojen säilyttämisestä sekä niiden poistamisesta ja arkistoinnista. Tämä voitaisiin mahdollisesti toteuttaa saman tyyppisesti kuin nyt on passi- ja henkilökorttilaissa säädetty tietojen elinkaaren hallinnasta.

Esitettyyn lakiin digitaalisesta henkilöllisyystodistuksesta ei ole erikseen otettu toteamusta rekisteröityjen oikeuksista kuten rekisteröidyn tarkastusoikeudesta. Näistä olisi syytä todeta esityskokonaisuudessa esimerkiksi viittaamalla poliisin henkilötietolakiin, jossa säädetään rekisteröidyn oikeuksien käyttämisestä poliisin ylläpitämiin tietoihin.

# Kustannukset

Poliisihallitus nostaa esiin huolen suunniteltavan kokonaisuuden vaikutuksista passin ja henkilökortin hintaan. Hallituksen esityksen luonnoksessa on esitetty, että kustannukset tullaan vyöryttämään passien ja henkilökorttien hintoihin. Kyseessä on passiin ja henkilökorttiin sisältyvä lisäpalvelu, joten valittu ratkaisu on lähtökohtaisesti perusteltu. Syntyvien kustannusten on arvioitu vaikuttavan passien ja henkilökorttien hintoihin korottavasti n. 5-7,5 €. Passien ja henkilökorttien hintoihin vaikuttavat monet tekijät eikä tästä voida vetää suoraa johtopäätöstä siitä, mikä tulee olemaan hakijalta perittävän käsittelymaksun suuruus.

Lupahintoihin jyvitettävien kustannusten osalta on myös syytä olla tarkka sen suhteen, että passien ja henkilökorttien maksuihin tulee huomioitavaksi vain sellaisia kustannuseriä, jotka suoraan syntyvät digitaalisen henkilöllisyystodistuksen tuottamisesta. Kustannuserät määriteltäneen käytännössä vuosittain kappalehinnoin, kuten nykyään toimitaan passilla ja henkilökortilla olevien DVV:n tuottamien varmenteiden osalta.

Poliisijohtaja Sanna Heikinheimo

Ylitarkastaja Juhani Ruutu

Asiakirja on sähköisesti allekirjoitettu asianhallintajärjestelmässä. Poliisi 14.04.2022 klo 14:18. Allekirjoituksen oikeellisuuden voi todentaa kirjaamosta.

Liitteet -

Jakelu VM kirjaamo

Tiedoksi Emilia Laitala / VM
Maarit Huotari / VM
Karl Linderborg
Poha / Esikunta