THALES

LAUSUNTO 16.2.2026

Otsikko: Lausuntopyyntö luonnoksesta hallituksen esitykseksi passilain ja henkilökorttilain muuttamisesta, diaarinumero ja linkki lausuntopyyntöön: VN/13936/2025

Taustaa: Sisäministeriö pyytää lausuntoa luonnoksesta hallituksen esitykseksi passilain ja henkilökorttilain muuttamisesta. Hallitus linjasi huhtikuun 2025 kehysriihessä Suomen passien enimmäisvoimassaoloajan pidentämisestä 10 vuoteen ottaen huomioon mahdolliset turvallisuustekijöistä aiheutuvat poikkeukset.

Passien ja henkilökorttien voimassaoloajan pidentäminen on teknisesti mahdollista. On kuitenkin tärkeä huomata, että mikäli muutos tehdään käytössä olevalle asiakirjatyypeille ilman muita toimenpiteitä, asiakirjojen väärinkäytön riski kasvaa huomattavasti. Voimassaoloajan kaksinkertaistaminen lisää asiakirjassa olevan sirun haavoittuvuusriskiä ja vaatimuksia asiakirjan ja sirun kestävyydelle.

Passien ja henkilökorttien voimassaoloajan pidentäminen heikentää sähköistä asiakirjaturvallisuutta ja lisää vaatimuksia sirun kestävyydelle. Kasvavat huolenaiheet kansallisen turvallisuuden, identiteettivarkauden ja kyberhyökkäysten osalta asettavat sähköisten henkilöllisyystodistusten myöntäjät tilanteeseen, jossa heidän on valittava mahdollisimman tulevaisuudenkestävä ja kyberresilientti ratkaisu luottamuksen perustaksi. Aiemmin painopiste oli kyberturvallisuudessa, eli kehitettiin suojattuja sulautettuja ohjelmistoratkaisuja, jotka suojasivat kaikilta siihen aikaan tunnetuilta hyökkäyksiltä. Turvallisuus kuitenkin usein heikentyy ajan myötä, kun mahdolliset hyökkääjät kehittyvät entistä taitavammiksi. Esimerkiksi kvanttitietokoneiden kehitys on riski siruturvallisuudelle. Kvanttitietokoneet voivat teoriassa ratkaista matemaattisia ongelmia, joihin nykyinen salaus perustuu. Tästä syystä perinteiset julkisen avaimen salausmenetelmät (esim. RSA, ECC) tulevat tulevaisuudessa alttiiksi murtamiselle. PQC (Post-Quantum Cryptography, suomeksi post-kvanttisalakirjoitus) tarkoittaa uusien salaustekniikoiden kokonaisuutta, joka on suunniteltu kestämään tulevien kvanttitietokoneiden murtautumiskyvyn. Kyberresilienssin käsite vie kyberturvallisuuden uudelle tasolle, keskittyen enemmän siihen, kuinka varmistetaan, että tuotetta voidaan käyttää turvallisesti koko suunnitellun elinkaaren ajan, myös haitallisten kybertilanteiden ilmetessä. Myös käytössä olevan asiakirjan sähköistä turvallisuutta saatetaan joutua parantamaan uusimpia hyökkäyksiä vastaan. Passien ja henkilökorttien siruissa on jo valmius sirun käyttöjärjestelmän päivittämiseen käytössä oleville asiakirjoille. Voimassaoloajan muutoksen yhteydessä tarve tämänkaltaiselle päivittämiselle tulee kasvamaan ja siihen tulee varautua.

Puollamme esitystä, että henkilökorttiin sisältyvän kansalaisvarmenteen voimassaoloaika rajataan viiteen vuoteen turvallisuussyistä. Lisäksi korostamme, että QSCD-tuotteen voimassaoloajan muuttamisessa kymmenvuotiseksi liittyisi merkittävä riski.

Schengen alueen sisällä myönnetty passi ja henkilökortti on lähtökohtaisesti houkutteleva väärennöskohde. Useat eri maiden rajaviranomaiset jakavat mielipiteen että noin viiden vuoden välein olisi hyvä päivittää asiakirjan turvallisuuskonsepti. Tämä johtuu siitä että jo noin kahden vuoden kuluttua uuden asiakirjan myöntämisesti, kentällä alkaa näkyä uskottavan kaltaisia väärennöksiä. Tästä syystä edellä mainittujen asiakirjojen uudelleensuunnittelu on tärkeä toteuttaa 10 vuotiseen voimassaoloaikaan siirryttäessä ja uudelleensuunnittelulle tulee varata riittävä siirtymäaika. Muutoin olisimme tilanteessa, jossa vuoden 2023 alussa julkaistu asiakirja olisi käytössä 19 vuoden päästä julkaisustaan. Tämä tekisi asiakirjasta entistä houkuttelevamman väärennöskohteen. Uudelleensuunnittelussa visuaalinen ilme uudistetaan ja

turvaominaisuudet korvattaisiin päivitetyillä turvaominaisuuksilla. Uudelleensuunnittelulle varattava aika on noin 15–18 kuukautta.

Voimassaoloajan maksimipituuden pidentäminen voi lisätä merkittävästi kausivaihtelua valmistus- ja toimitusmäärissä. Mikäli tavoitteena on säilyttää nykyisenkaltainen toimitusnopeus sekä toimitusverkosto, on tärkeää minimoida tämä ilmiö. Yksi vaihtoehto kausivaihtelun tasaamiseen on viisi ja kymmenen vuotta voimassa olevien asiakirjojen myöntäminen rinnakkain ylimenokauden ajan.

Ehdotetun 2 momentin pääsäännön mukaan hakijan kasvokuvan saisi ottaa vain sellainen elinkeinonharjoittaja tai oikeushenkilö, jonka kaupparekisterilain (564/2023) 4 §:ssä tarkoitettu toimiala tai tarkoitus on valokuvaustoiminta. Tämänlaisen menettelyn valvonta on työlästä, eikä se lisää prosessin turvallisuutta merkittävästi. Väärän kuvan käyttämisen lisäksi morphing eli kuvamuuntelu luo merkittävän riskin prosessiin. Morphing tarkoittaa digitaalisessa kuvankäsittelyssä ja biometrisissä järjestelmissä kuvien saumakasta muuntamista tai sulauttamista toisiinsa. Morphing-väärennöksellä viranomaiselle toimitettu kuva voidaan muokata siten, että se hyväksytään useamman eri henkilön kasvoina. Tämä mahdollistaa esimerkiksi usean henkilön käytön samalla asiakirjalla, mikä vaarantaa henkilöllisyydenvarmennuksen luotettavuuden.

Edellä mainituiden syiden takia valokuvaaminen kannattaa järjestää passi- ja/tai henkilökorttihakemuksen jättötilanteessa viranomaisen valvonnassa. Tämä takaa turvallisemman, tehokkaamman ja helpomman palvelupolun kansalaiselle. Lisäksi voidaan varmistaa, että valokuvat täyttävät aina voimassa olevat viranomaisvaatimukset. Toiseksi prosessin keskittäminen poliisin toimipisteeseen mahdollistaa henkilötietojen kokonaisvaltaisen suojauksen. Kokonaisvaltainen end-to-end-tietoturva varmistaa, että henkilökohtaista tietoa käsitellään luotettavasti jokaisessa vaiheessa. Kolmanneksi palvelun saavutettavuus paranee, kun kaikki ID- ja matkustusasiakirjoihin liittyvät toiminnot hoidetaan yhdellä käynnillä poliisin tiloissa. Tämä sujuvoittaa hakemusprosessia ja vähentää virheiden mahdollisuutta. Kansalaisen ei tarvitse asioida erikseen valokuvaamossa, mikä säästää aikaa ja vaivaa.

Valokuvan ja samalla muiden biometristen tunnisteiden kuten sormenjälkien rekisteröinti voidaan järjestää esimerkiksi viranomaisen tiloissa olevilla rekisteröintikioskeilla. Rekisteröintikioskit hyödyntävät kehittyneitä ja valvottuja biometrisiä ohjelmistoja. Tämä takaa, että henkilöllisyys voidaan varmistaa luotettavasti ja tehokkaasti sekä minimoida identiteettihuijauksen ja asiakirjaväärennösten riskit. Kuvien ottaminen suoraan rekisteröintikioskilla tarkoittaa, ettei kuvia tarvitse toimittaa erikseen, mikä pienentää tietosuojariskejä sekä estää kuvien mahdollisen väärinkäytön.