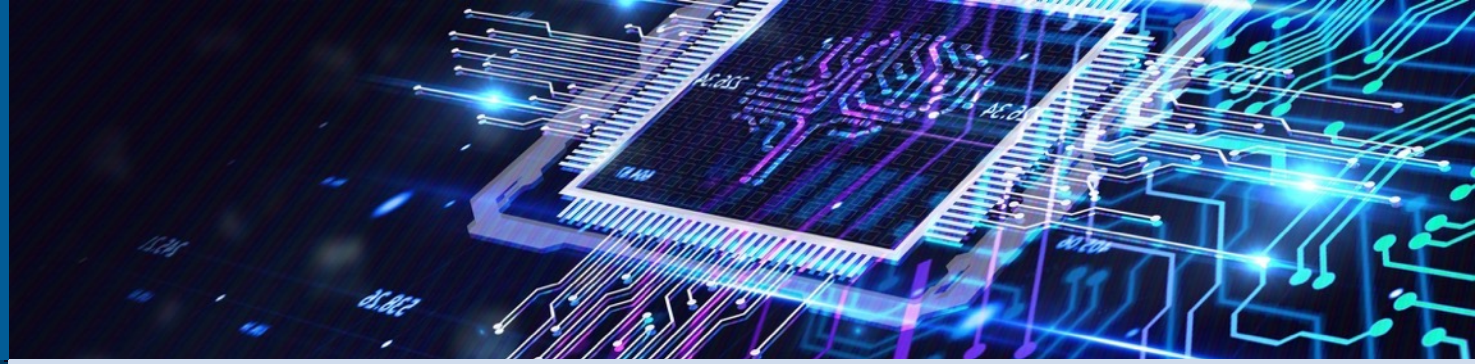
CSC

ICT Solutions for Brilliant Minds



Katsaus henkilön sähköiseen tunnistamiseen koulutustoimialalla

25. toukokuuta 2023, Manne Miettinen

Käsitteet: (Sähköinen) identiteetti

- Käyttäjää kuvaavien tietojen joukko tietokannoissa
  - id = 12345,
  - etunimi = Ella, sukunimi = Esimerkki, rooli = oppija, oppilaitos = Mäntymäen koulu
- Identiteetin ydin on *yksilöivä tunniste*, joka erottaa käyttäjän yksiselitteisesti muista käyttäjistä (yksilöinti eli identification) ja voi toimia avaimena eri rekisterien välillä
  - Toimialalla mm. oppijanumero, hetu, eppn, CryptID, …
- Identiteetinhallinnan keskeiset toimintaprosessit liittyvät sähköisen identiteetin luomiseen, päivittämiseen ja poistamiseen

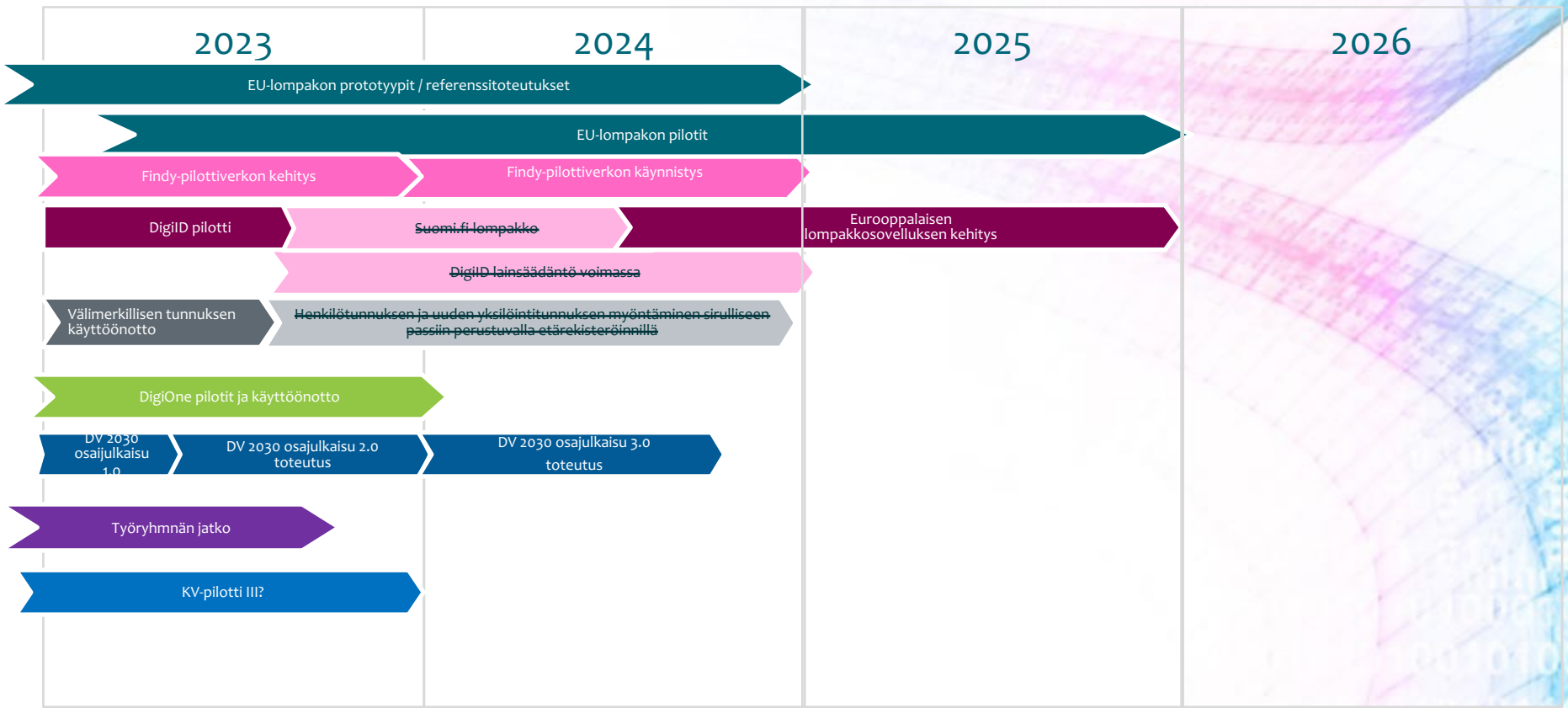
Käsitteet: Autentikointi eli identiteetin todentaminen

- Keinot, jolla sähköiseen palveluun kirjautuva henkilö voidaan varmistaa tietyn yksilöivän tunnisteen haltijaksi
- Yleensä perustuu johonkin seuraavista
  - Jotain mitä henkilö tietää tai muistaa (esim. salasana)
  - Jotain mitä henkilöllä on hallussaan (esim. toimikortti)
  - Jotain mitä henkilö on (esim. sormenjälki)
- Keskeinen (organisatorinen) haaste on ensitunnistus eli toimenpiteet, joilla henkilöllisyys todennetaan identiteetin luomisvaiheessa

Toimialan käyttäjähallintoratkaisut

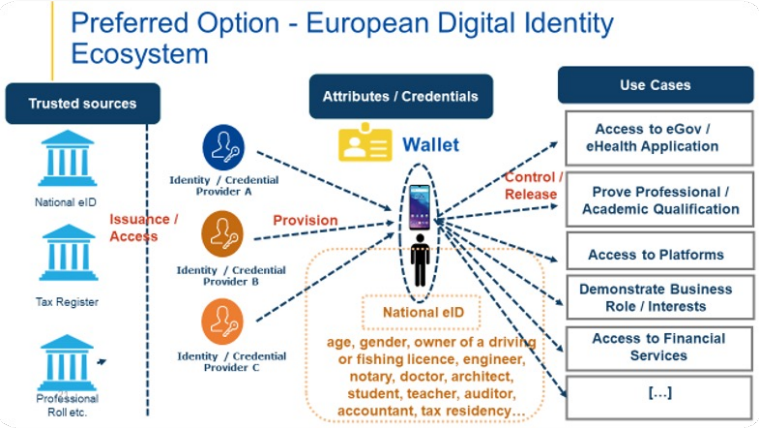
- Tietojärjestelmäkohtaiset erillistunnukset ja salasanat
  - Kussakin järjestelmässä erillinen identiteetti
- Kansalaisen suomi.fi-tunnistus
  - Identiteetti perustuu Väestötietojärjestelmään
- Haka-luottamusverkosto
  - Identiteetti perustuu korkeakoulun henkilörekisteriin
  - Noin 460 palvelua, 60 miljoonaa kirjautumista 2022
- MPASSid-luottamusverkosto
  - Identiteetti perustuu O/K-järjestäjän henkilörekisteriin
  - Noin 50 palvelua, 15, 3 miljoonaa kirjautumista 2022

Identiteetinhallinnan isojen hankkeiden kokonaiskuva

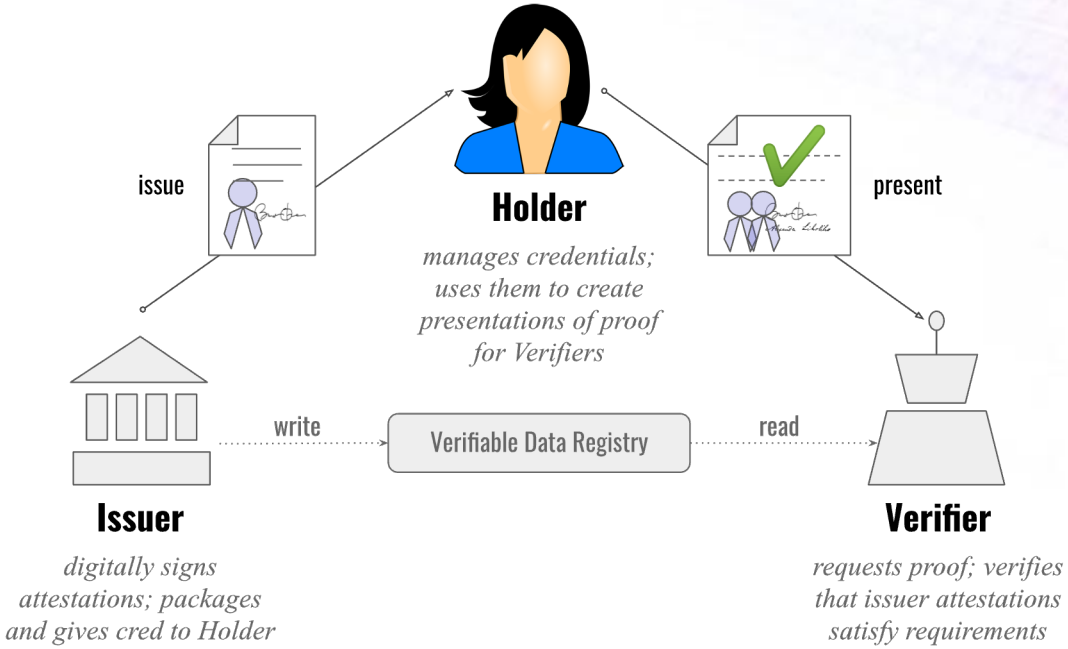


Digitaaliset lompakot ja vahvistettavat tiedot

- Jäsenvaltioiden tulee tarjota digitaalinen lompakko kansalaisilleen ilmaiseksi
- Digitaalisia lompakoita voivat tarjota (a) jäsenvaltiot, (b) jäsenvaltion mandaatilla, (c) itsenäisesti, mutta jäsenvaltion tunnustamana.
- Implementaatiot harmonisoidaan yhteisillä vaatimuksilla ja standardeilla (toolbox)
- Implementaation takaraja on 12kk säädöksen voimaantulon jälkeen
- Vahvistettavilla tiedoilla on sama juridinen asema kuin notarisoiduilla dokumenteilla



Itsehallittavan identiteetin malli ja toimijat



Luottamusverkostot ja identiteettilompakko

OMINAISUUS	LUOTTAMUS-VERKOSTO	IDENTITEETTI-LOMPAKKO	LOMPAKON HYÖDYT
Käyttöliittymä	Verkkoselain	Lompakkosovellus	Käyttäjä hallitsee tiedon Rajattu julkituonti
Tiedon luotettavuus	Kotiorganisaation tunnistuspalvelu	Lompakon haltija ja VDR	Tiedon tuottaja ei osallistu suoraan
Käyttäjän toimien seuraaminen	Tunnistuspalvelu ja asiointipalvelu	Mahdollista estää	Tietosuoja, GDPR
Luottamusmalli	Luottamusverkoston sopimus, PKI, metadatan allekirjoitus	VRD, tietokanta, ZKP	Joustavuus, skaalautuvuus

Digivisio 2030 tunnistuksenvälityspalvelu

- Tunnistuksenvälityspalvelu, joka välittää suomi.fi/Haka/MPASSid -tunnistusta, ja on kytketty OPH:n oppijanumerorekisteriin
- Tulevaisuudessa käyttö mahdollista myös muihin kuin Digivision palveluihin tunnistautumiseen
- Koulutusasteesta ja –organisaatiosta riippumaton tunnistus

Passwordless Authentication

- Passkey on keino tunnistautua verkkopalveluun ilman salasanaa delegoimalla tunnistaminen esim. älylaitteen kasvojentunnistukselle.
- Google lanseerasi toukokuussa Passkey-tuen palveluihinsa
  - https://developers.google.com/identity/passkeys
- Käyttäjän älylaitteelle tallennetaan digitaalinen tunniste, jonka älylaitteen käyttöjärjestelmä tai verkkoselain osaa antaa oikealle palvelulle tunnistettuaan käyttäjän.