

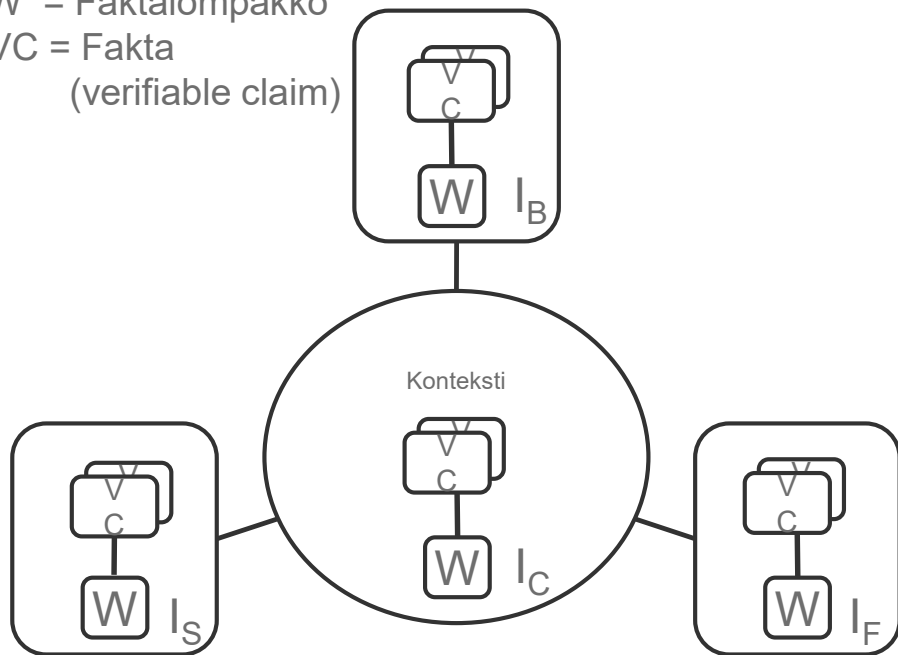
Digitaalisten identiteettien omistamien digitaalisten faktojen käyttö digitaalisissa konteksteissa

DRAFT

timo.hotti@op.fi

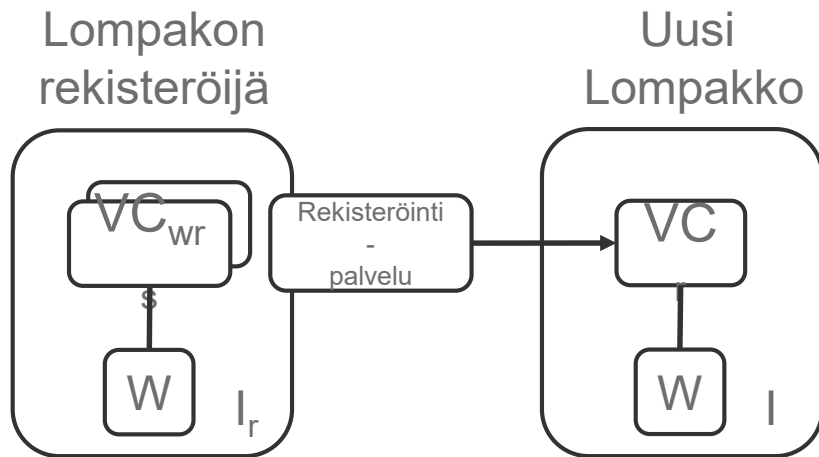
Findyn yleinen käyttötapaus - Luotettavan datan käyttö arvoa luovassa kontekstissa

I = Identiteetti
W = Faktalompakko
VC = Fakta
(verifiable claim)



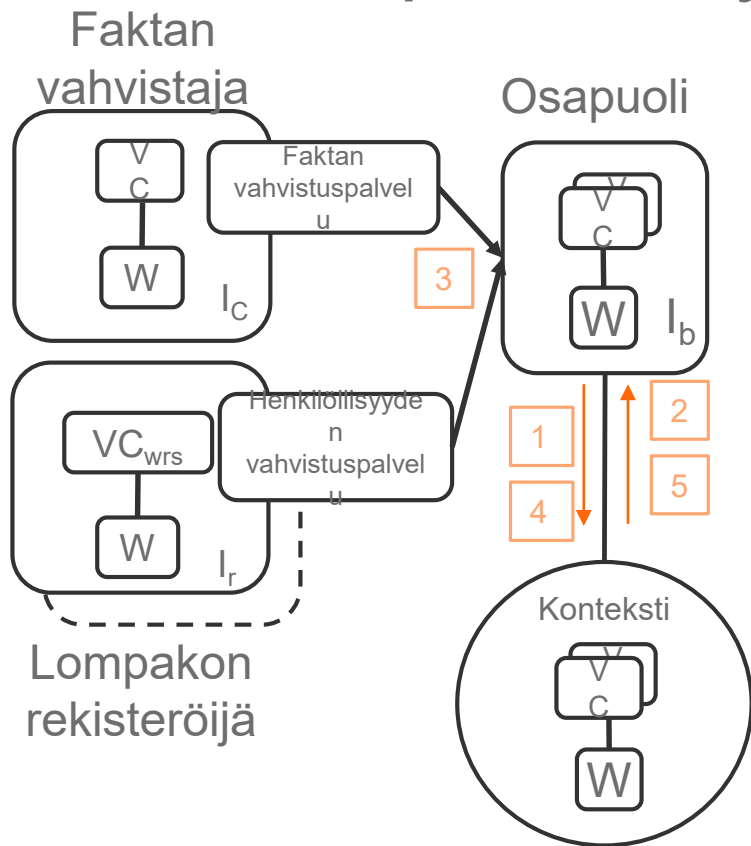
- Findy-verkon tarkoitus on poistaa arvoa luoviin identiteettien väliin prosesseihin liittyvää kitkaa
 - Arvo syntyy käyttök kontekstissa, joka hyödyntää osapuolten esittämiä faktoja
- Identiteetit (kansalaiset, organisaatiot) käyttävät faktalompakostaan löytyviä faktoja eri konteksteissa
 - Faktojen käyttö kontekstissa synnyttää tyypillisesti uusia faktoja, esim. sopimuksia
- Myös kontekstin pitää pystyä esittämään itsestään faktoja, joiden perusteella kontekstiin osallistujat voivat luottaa siihen
 - Mitä kontekstissa tehdään, kuka siitä vastaa, kuka sitä valvoo...
- Luottamus kontekstin ja sen osapuolen välillä muodostuu kahdesta osasta:
 - "Kuka minä olen" – lompakon omistajuus
 - "Mitä minä olen" - lompakon sisältö, esim. lasku, luottoluokitus, takaussitoumus, tilauskanta...
- Kontekstissa käytettyjen faktojen vahvistamisen luoma lisäarvo sekä niihin liittyvät vastuut pitää pystyä hinnoittelemaan käyttök kontekstiin sopivalla tavalla

”Kuka minä olen” – Faktalompakon rekisteröinti omistajalleen



- Uusi lompakko pitää liittää omistajaansa luotettavalla rekisteröintiprosessilla
 - ”ensitunnistus” / ”todentaminen”
- Rekisteröintiprosessin tuloksena lompakkoon muodostuu ”ankkuroitu” fakta siitä, kuka lompakon omistaa
 - OP on suunnitellut FIDO2-pohjaisen prosessin
- Rekisteröintiprosesseja voivat tarjota kaikki sellaiset tahot, jotka kykenevät riittävän luotettavaan todentamiseen ja tuohon todennukseen liittyvän faktan myöhempään vahvistamiseen
- Rekisteröintejä voidaan tehdä useita per lompakko
 - Yksi per ”pysyvä DID”
- Rekisteröijä voi myöhemmin vahvistaa käyttökonfektikohtaisesti ”kuka minä olen” –

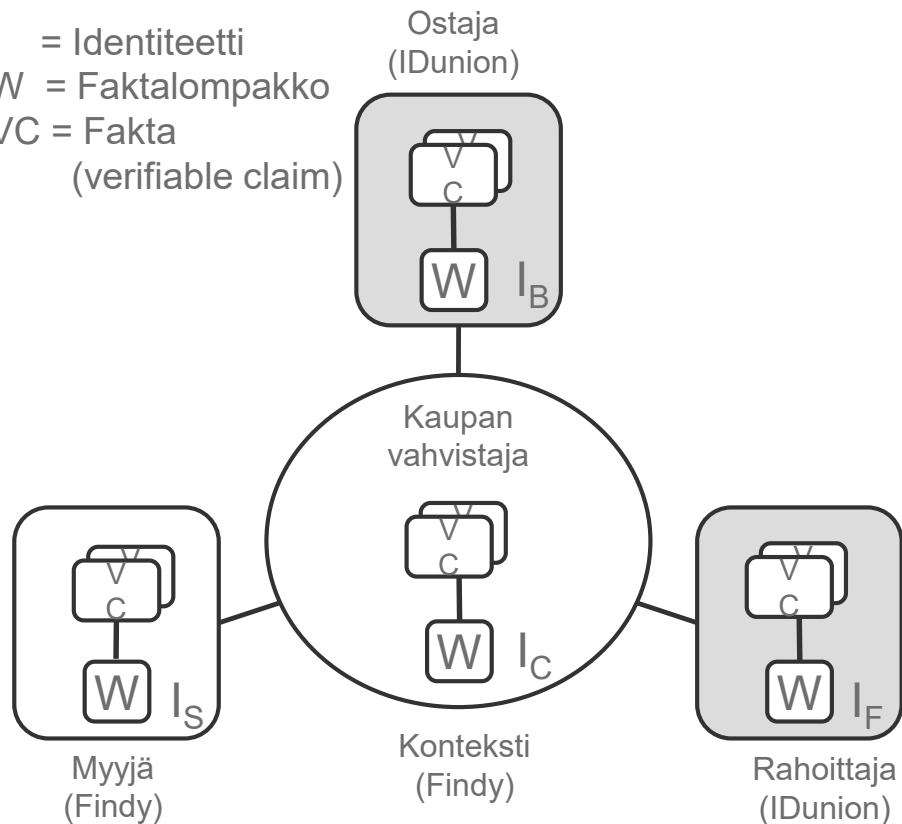
”Kuka ja mitä minä olen” – Faktalompakon käyttö kontekstissa



1. Lompakon omistaja esittää itsestään yhden tai useamman ”mitä minä olen” -tyyppisen faktojen käyttökotekstille, mutta ei yhtään ”kuka minä olen” -faktaa
2. Käyttökoteksti esittää esitetyille faktoille korotetun vastuuvaatimuksen sekä vaatimuksen vähintään yhdestä vahvistettavasta ”kuka minä olen” -faktasta
3. Lompakon omistaja hakee kontekstiin sidotun (maksullisen) vahvistuksen ”kuka minä olen” -faktalle sekä muille korotetun vastuuvaatimuksen alaisille ”mitä minä olen” -faktoille
4. Lompakon omistaja esittää pyydettyjä korotetun vastuuvaatimuksen täyttävät faktat kontekstille
5. Konteksti finalisoi tapahtuman sekä siihen liittyvät sopimukset ja maksut

Yhteensopivuus eri SSI-verkkojen välillä

I = Identiteetti
 W = Faktalompakko
 VC = Fakta
 (verifiable claim)



- ToIP:n tekniset standardit määrittävät teknisen yhteensopivuuden, jonka avulla osapuolet voivat kommunikoida keskenään
 - DID, Verifiable Claims, ...
- Konteksti määrittää ne vaatimukset, jotka kontekstiin osallistuvien tahojen pitää täyttää pystyäkseen toimimaan kontekstissa
 - Konteksti voi esim. kelpuuttaa "henkilöllisyystodistukseksi" sekä Findystä-lompakosta löytyvän DVV:n issuoiman claimin että IDUnion-lompakosta löytyvän saksalaisen viranomaisen issuoiman claimin
 - Yleisesti käytettyjen claimien standardointi esim EU-tasoisena viranomaistyönä helpottaa yhteensopivuuden saavuttamista
 - Viranomaisasiointi on konteksti muiden joukossa
- Konteksti määrittää myös sen, millainen vastuu kunkin osapuolen esittämiin faktoihin liittyy