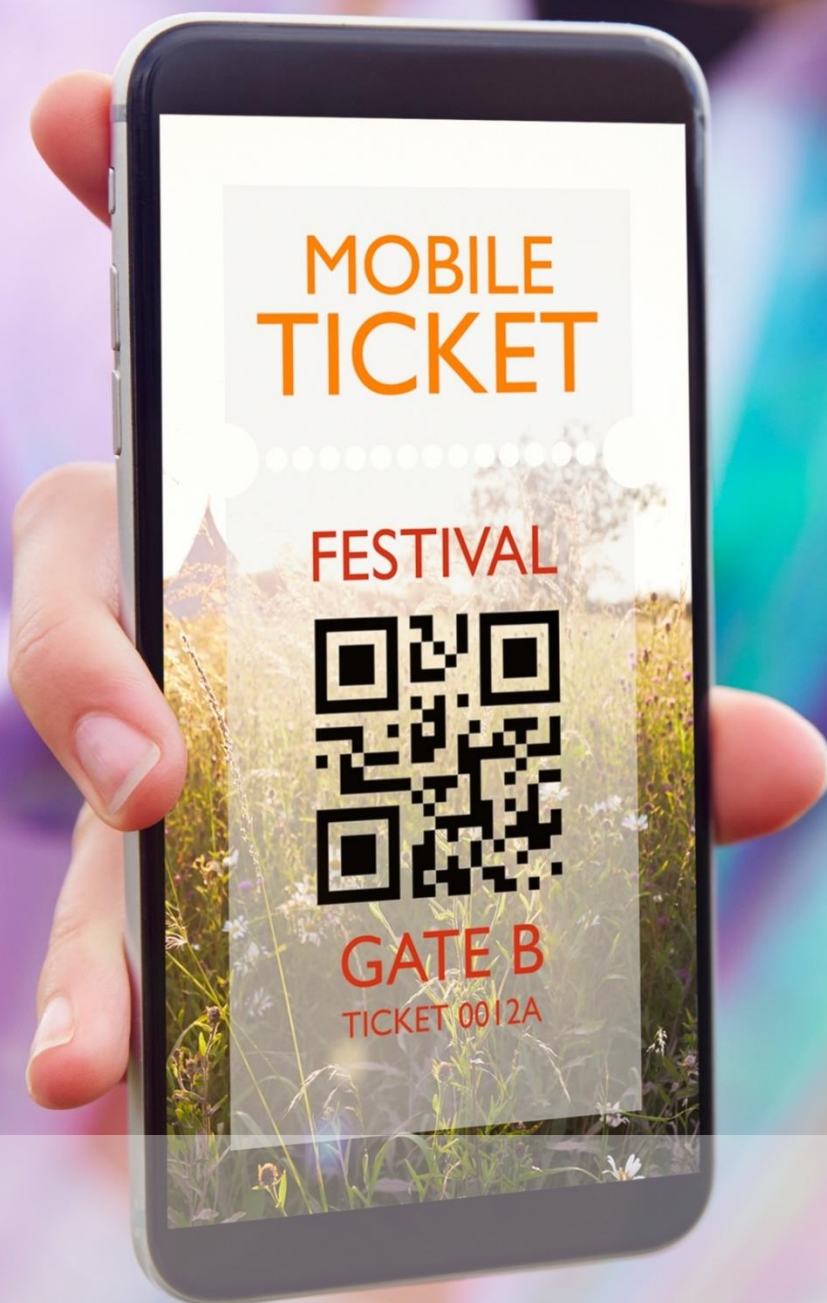


Korleis virkar EU si digitale identitetslommebok?





Kva kan du bruke lommeboka til

- **Logge inn:** Enklare tilgang til offentlege og private tenester på nett.
- **Lagre og dele/vise** digitale bevis som alder, førarkort, reseptar, attestar, utdanningsbevis, billetter mm.
- **Trygg handel:** Kjøpe, bestille og leie varer og tenester.
- **Signering:** Elektronisk, juridisk bindande signering.

Gratis eID til alle
Styrkar personvernet
Lanserast i Noreg innan 2030



Om oss

Jørgen Binningsbø

Sjefsarkitekt for nasjonale
fellesløysingar

Aamund Bremer

Arkitekt som jobbar med Digdir sine
tillitstenester.



Dette vil vi snakke om

- Kva er eIDAS 2.0 ?
- Kort introduksjon til digitale lommebøker
- EU sitt lommebok-økosystem
- Nasjonal sandkasse for digital lommebok



Om eIDAS-forordninga

- Innført i 2014
- Formål: «fri flyt av digital tenester»
- Regulerer eID og tillitstenester
- Stort sett basert på frivilligheit, og har **ikkje** ført til auka utbredelse eller bruk av eID i Europa



eIDAS2 stiller strengere krav

- **Tvungen utstedelse** av digitale ID-lommebøker i kvart medlemsland
- Tvungen aksept frå alle **andre medlemsland**
- Tvungen aksept frå **sentrale private tenestetilbydarar**
- Tvungen samsvar med **referansearkitekturen**



Lommebøker for virksomheter

- Forenkling og effektivisering for næringslivet
- Sikker og kontrollert datadeling
- Økt konkurranseevne og innovasjon
- Tillit og sikkerheit i digitale prosessar

Nytt lovutkast kjem i Q4

Arbeid med forskrifter og arkitektur i 2026



Introduksjon til digitale lommebøker




**The wall
around Wallet.**




**It's not a wallet.
It's Google Wallet.**

[Visit Google Wallet](#)

 [Download](#)

Only available on Android

sto
Hjem / Endelig leg på mobilen!

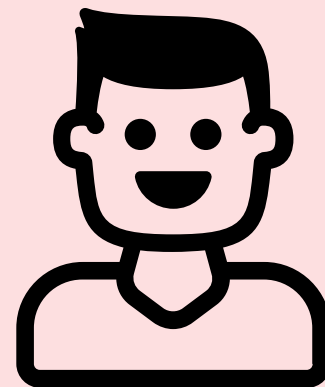
Endelig leg på mobilen!

Med ID-kort i BankID-appen kan du la passet ligge hjemme når du skal på Vinmonopolet og Posten – og når du skal inn på et utested hvor de har ordensvakter fra PSS Securitas i døra.

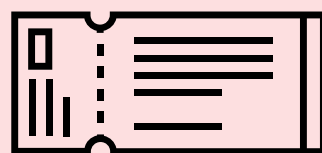
- ✓ Enkel aktivering med pass eller nasjonalt ID-kort
- ✓ Vis personlig QR-kode som skannes i kassen
- ✓ En tjeneste fra Stø, levert av samme selskap som BankID

 **Microsoft**
Microsoft Entra Verified ID

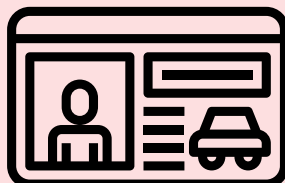




Flybilletter



Førarkort



Skattemelding



Lommeboka
fylles med ulike
bevis

Digital lommebok

Offentlig eID

Bevis

Bevis

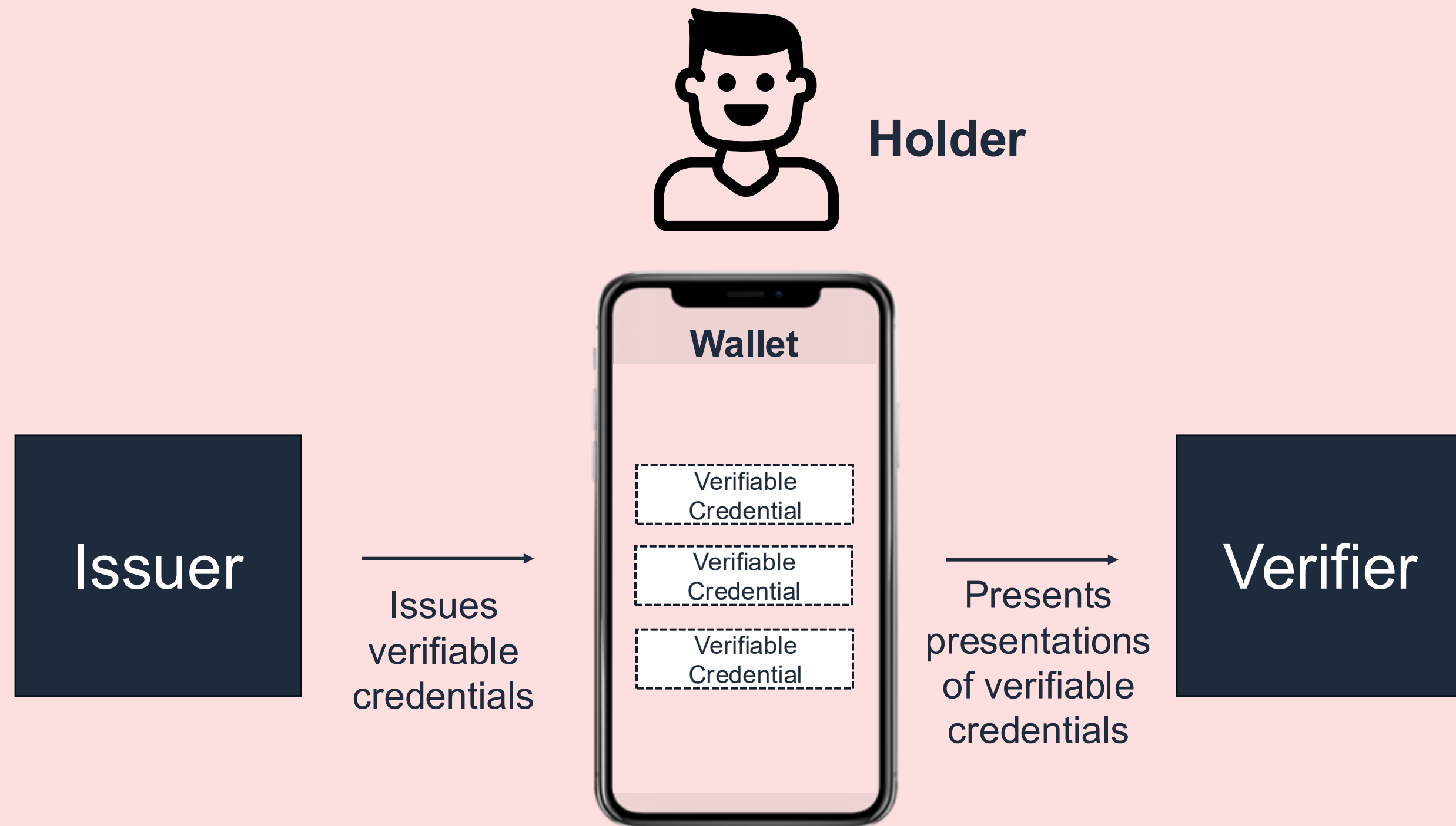
Bevis

Lommeboka
brukt for å få
tilgang til teneste

Digital teneste

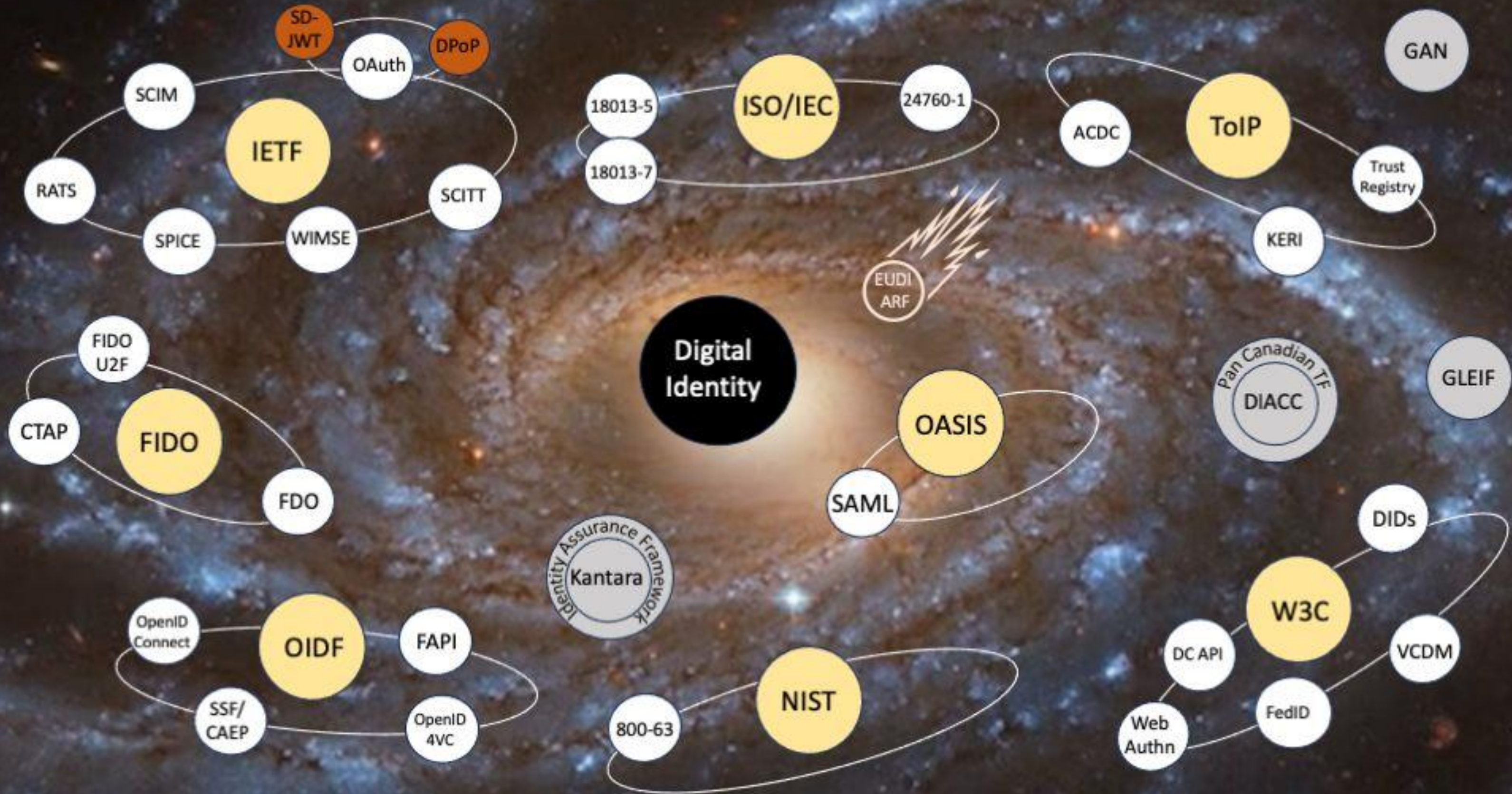


Brukar får tilgang til ei
digital lommebok med
ein norsk, offentlig eID
på høgt sikkerheitsnivå



Viktige eigenskapar ved digitale bevis

- **Kryptografisk verifiserbare**
 - Brukerstader kan verifisere at bevisa kjem frå ein gyldig utsteder
- Ein deler **presentasjonar** av bevisa.
 - Åpner for «selektiv deling». Attributter frå fleire bevis kan kombinerast i ein presentasjon
- **Holder binding** gir eintydig kobling mellom bevis og bruker
 - Kan realiserast gjennom kryptografi, biometri eller være attributt-basert
- **Revokasjon og reutstedelse**
 - Viktig ved «praktisk bruk» av bevis. Er støtta i EU-arkitekturen



Teknologivalg i EU-lommeboka

Protokollar for utstedelse og presentasjon	OpenID for Verifiable Credential Issuance (OpenID4VCI) OpenID for Verifiable Presentation (OpenID4VP)
Dataformat for bevis	ISO 18013-5 MDOC og SD-JWT-VC
Tillitsrammeverk	PKI / X.509 basert, ETSI TS 119 612 for tillitslister

EU Digital Identity Wallet (EUDIW)



Egenskapar me skal sjå på

- **Økosystemet**

- Tillitsmodell
- Lommeboka
- Deling av bevis
- Personvern

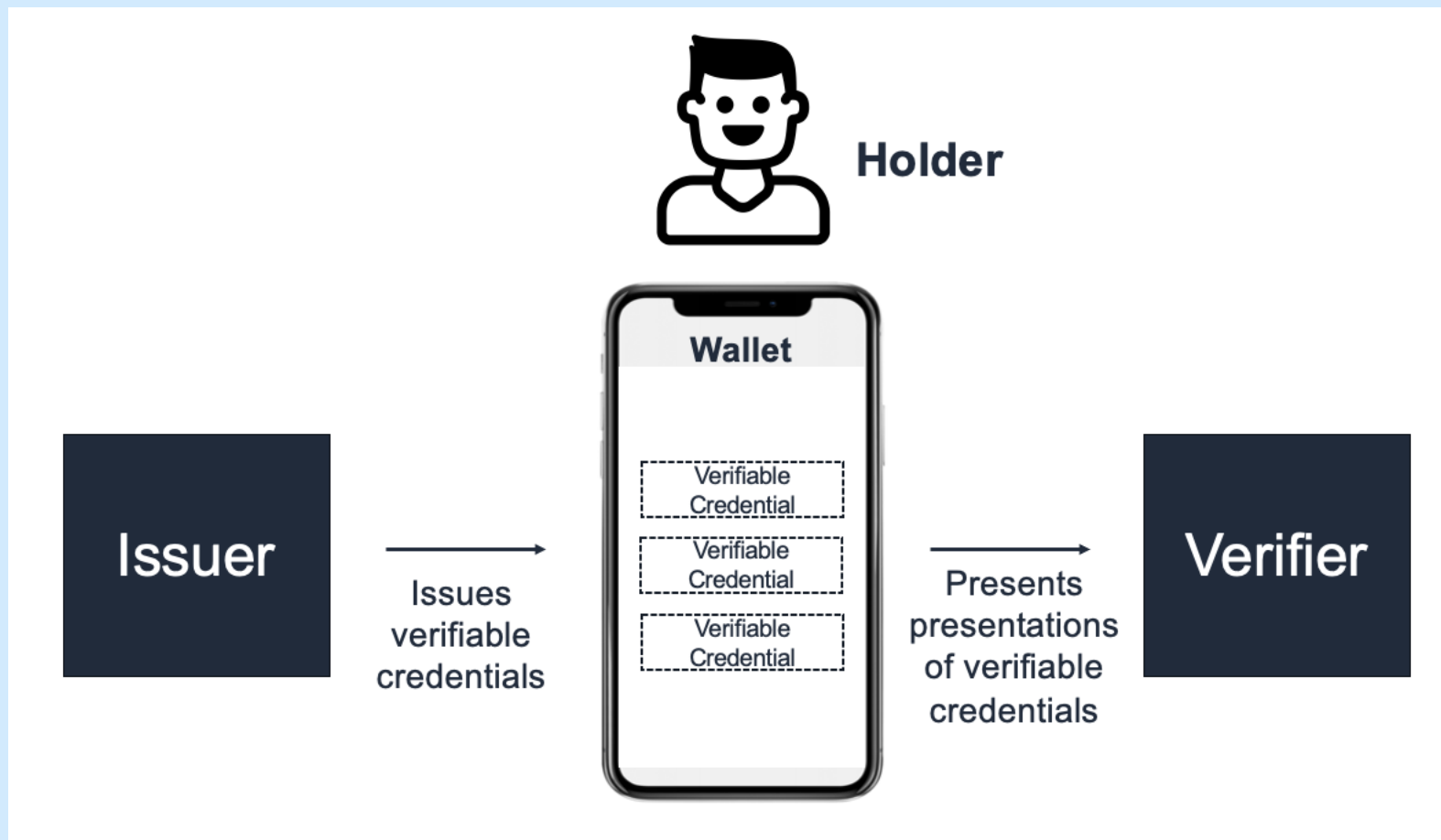


Lommeboka er eit stort økosystem



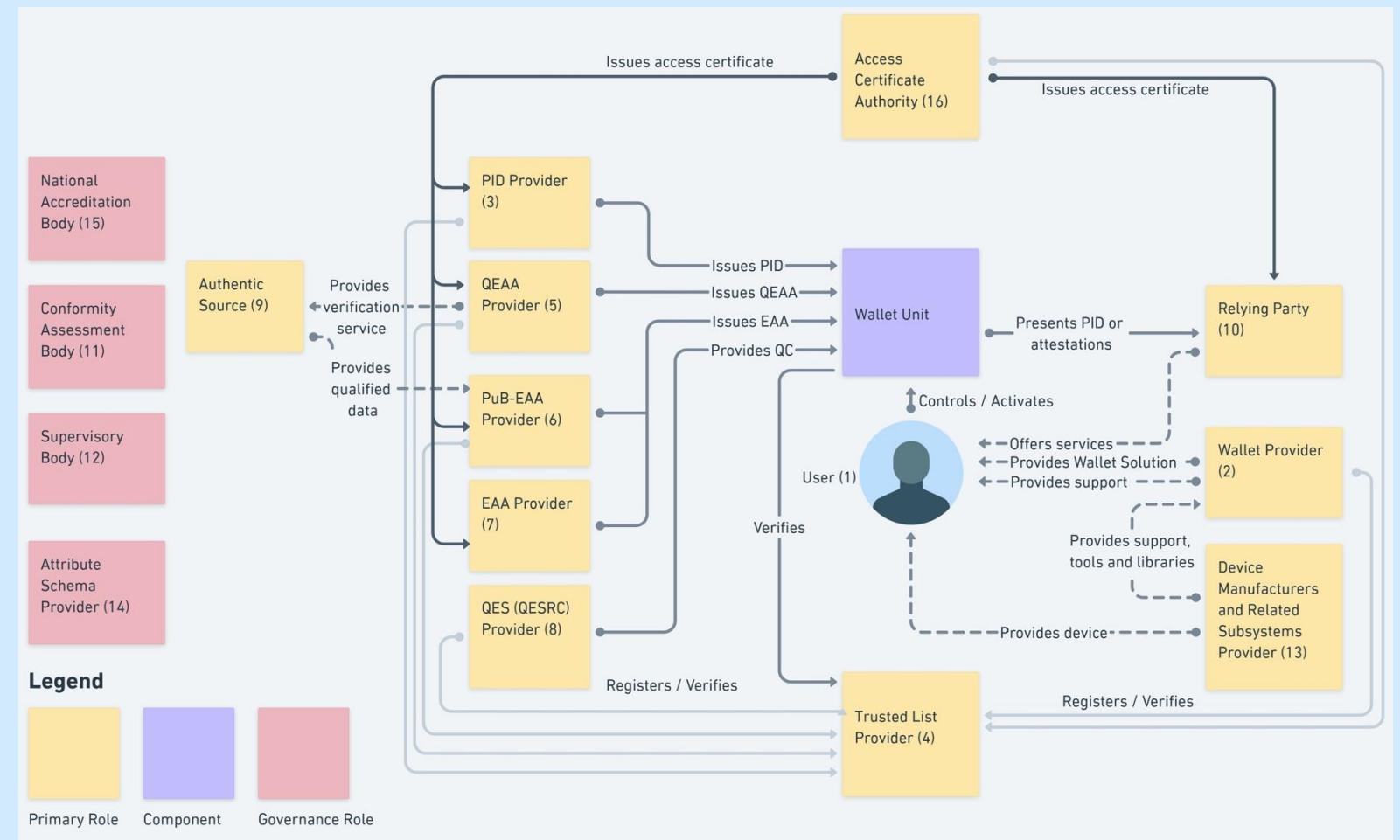
Ope tilgjengeleg på [Github](#)

Lommeboka er eit stort økosystem

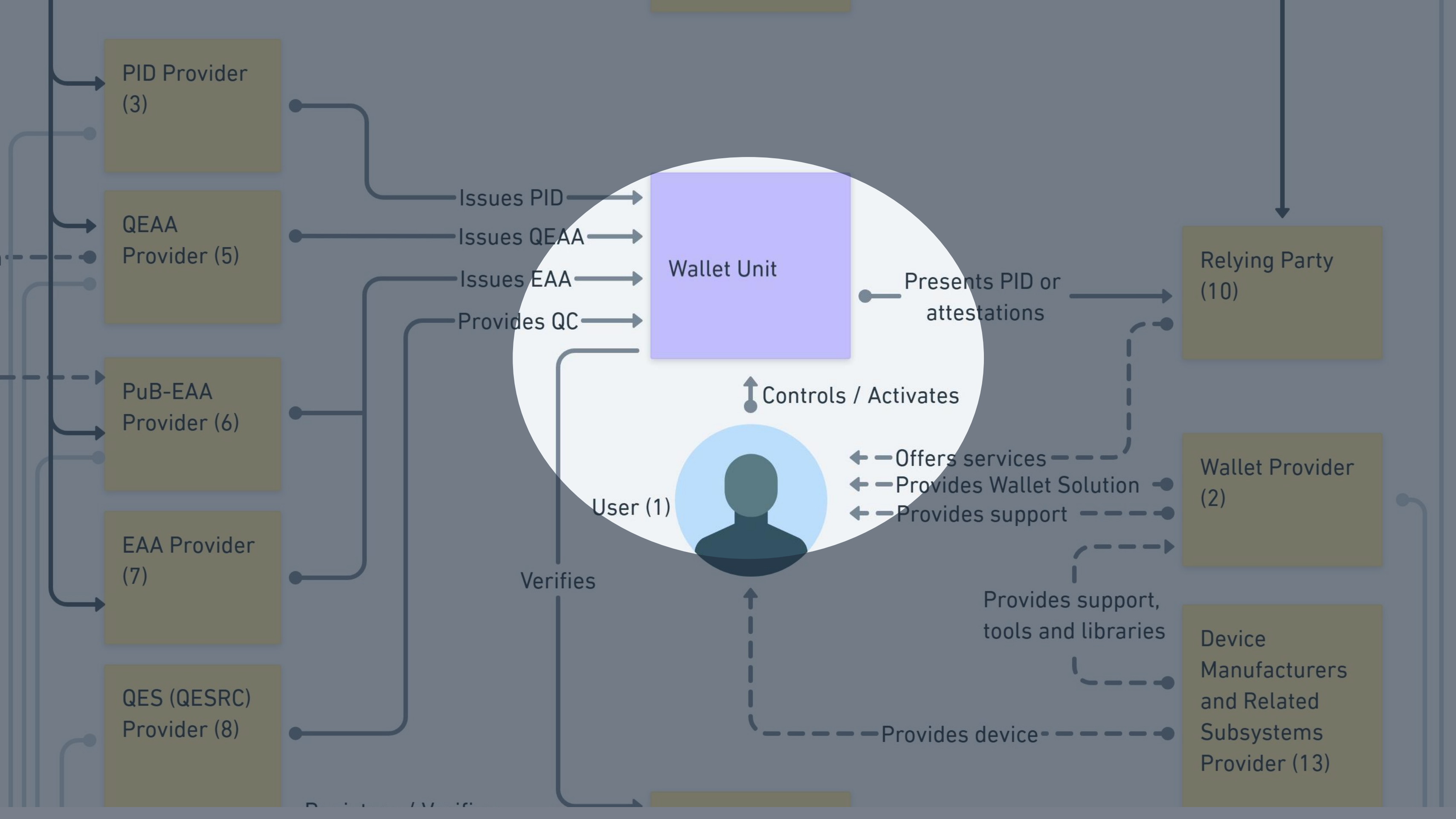


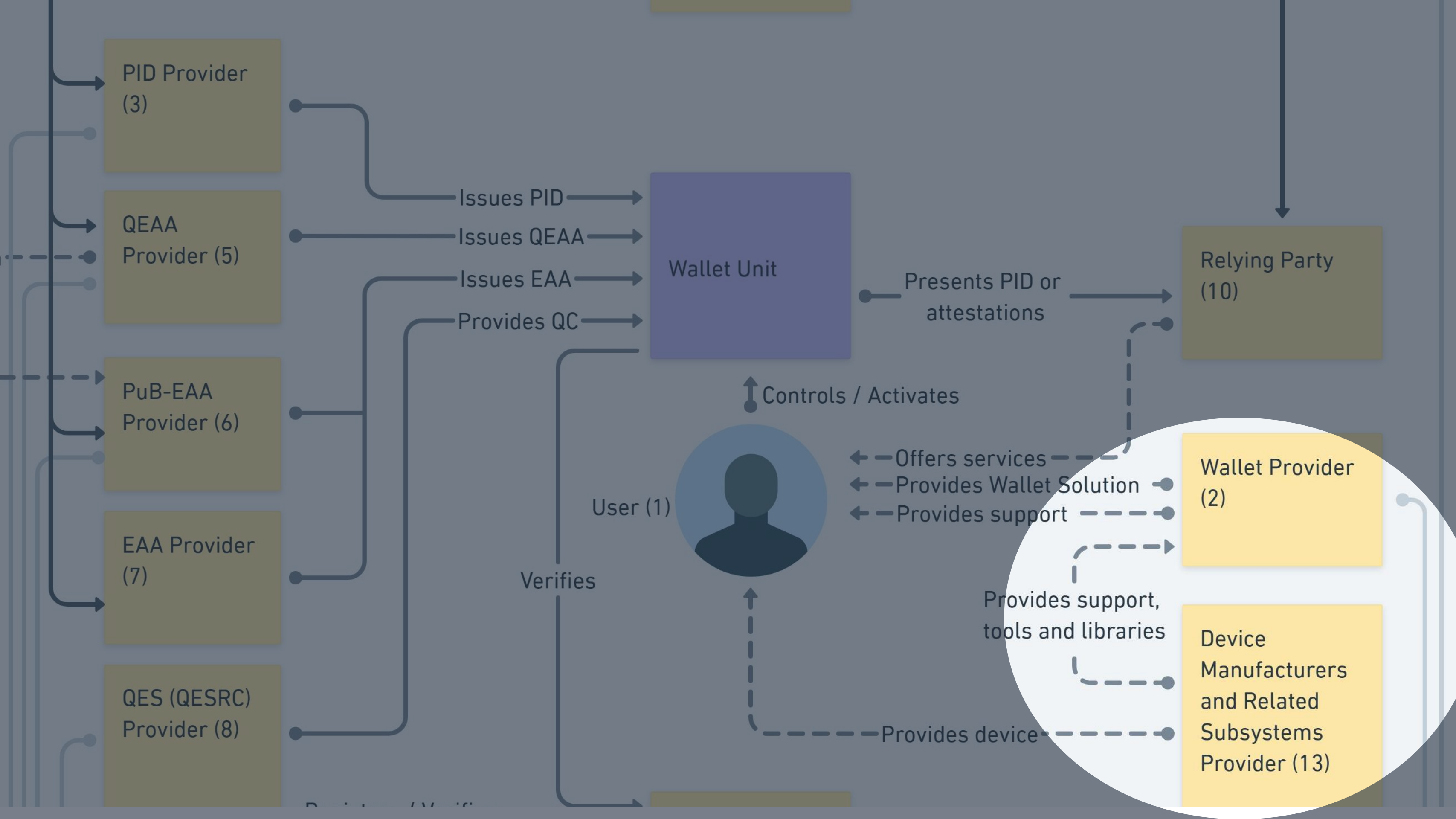
Lommeboka er eit stort økosystem

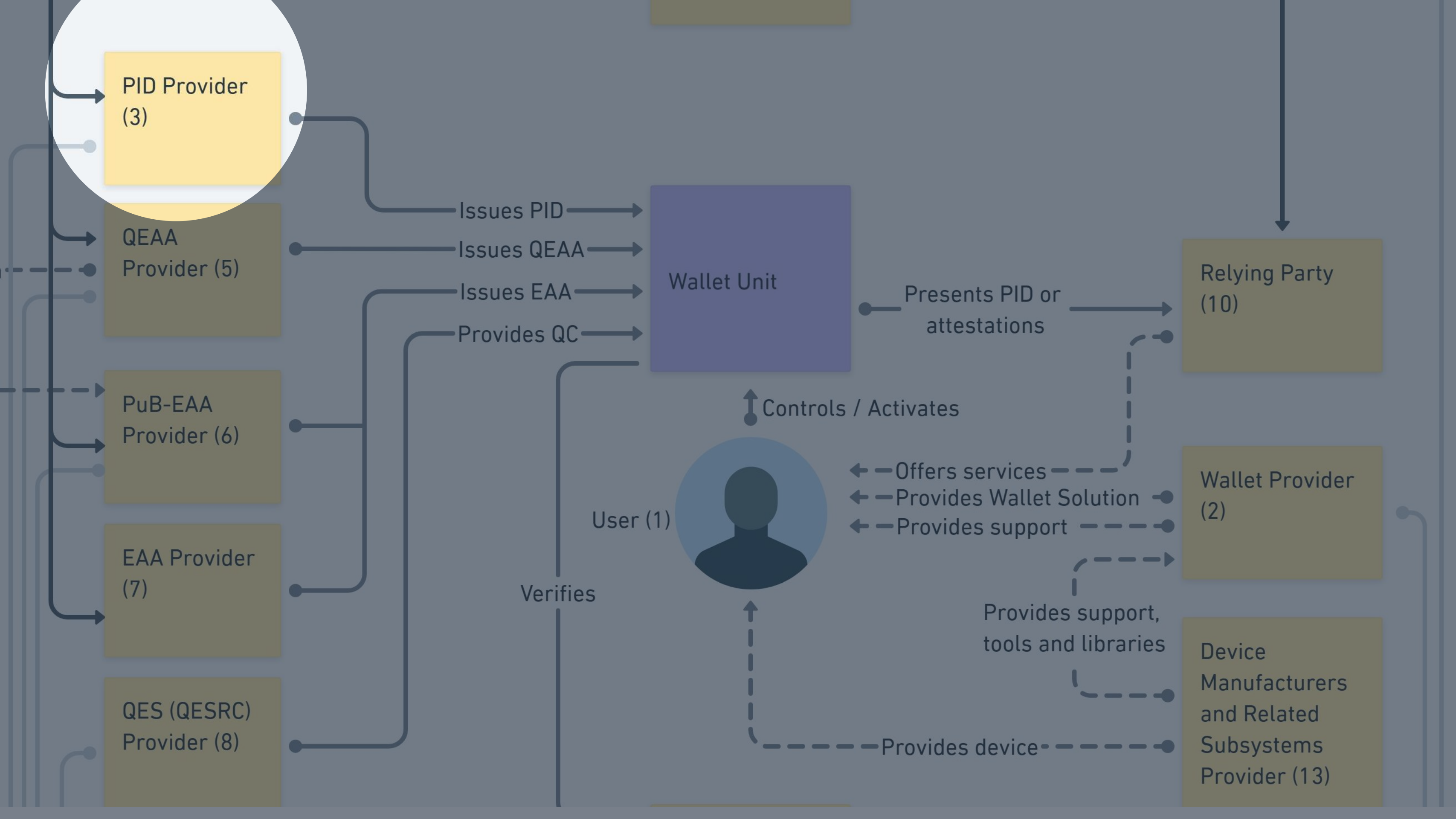
- 15-20 ulike roller
- Strengt sikkerheits- og sertifiseringskrav til kjernekomponentane

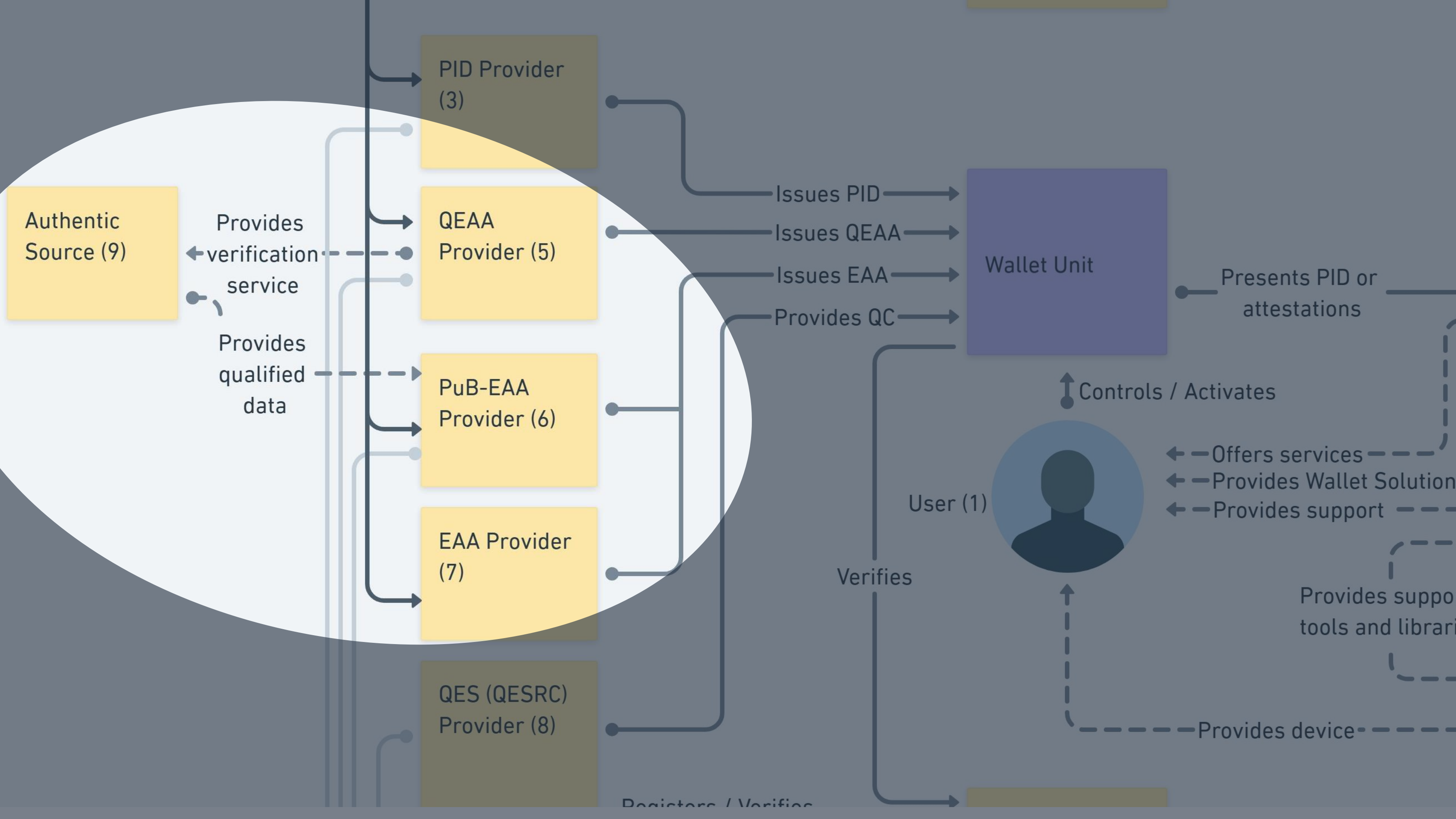


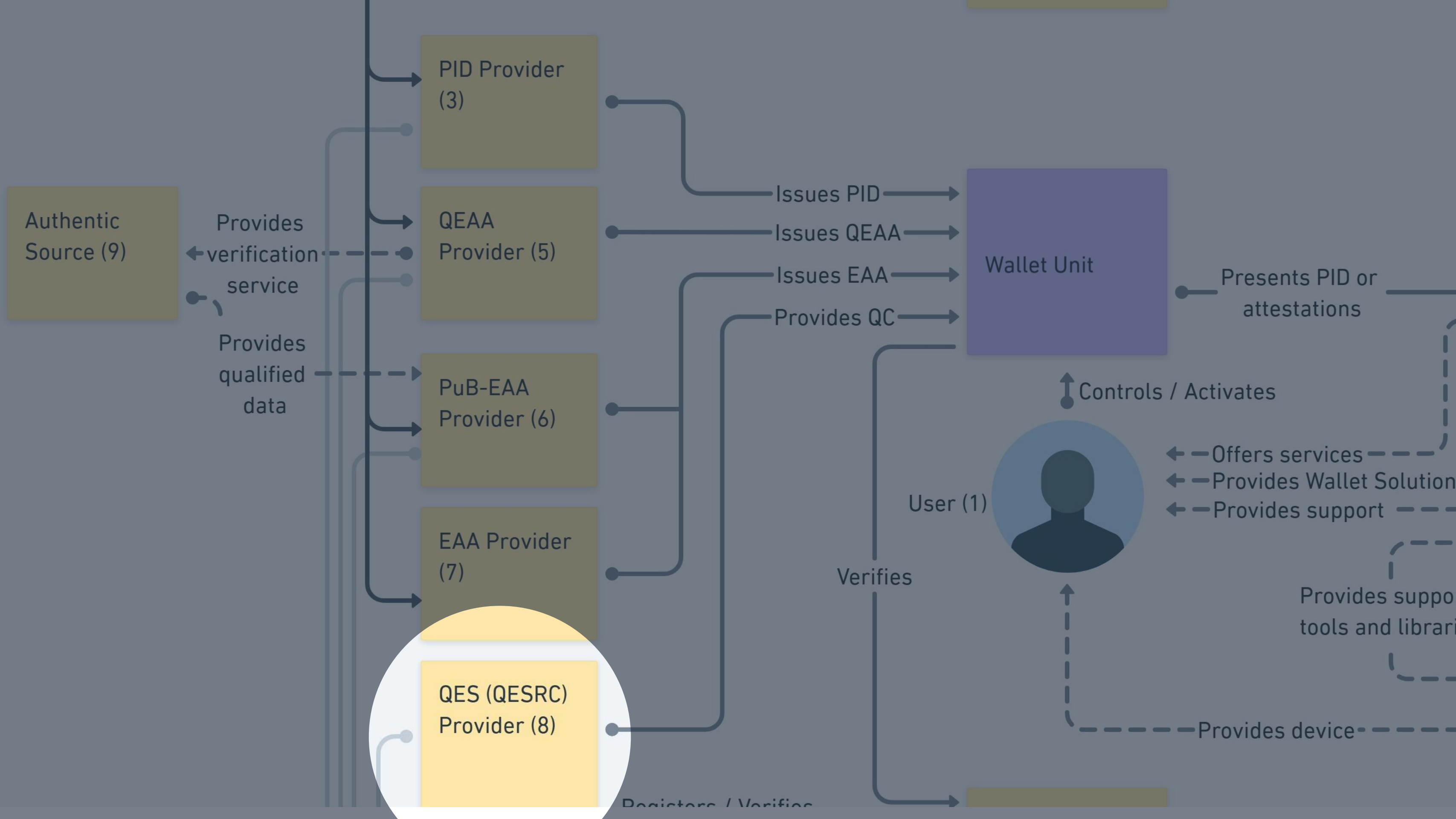
[ARF kap 3: EUDI ecosystem](#)

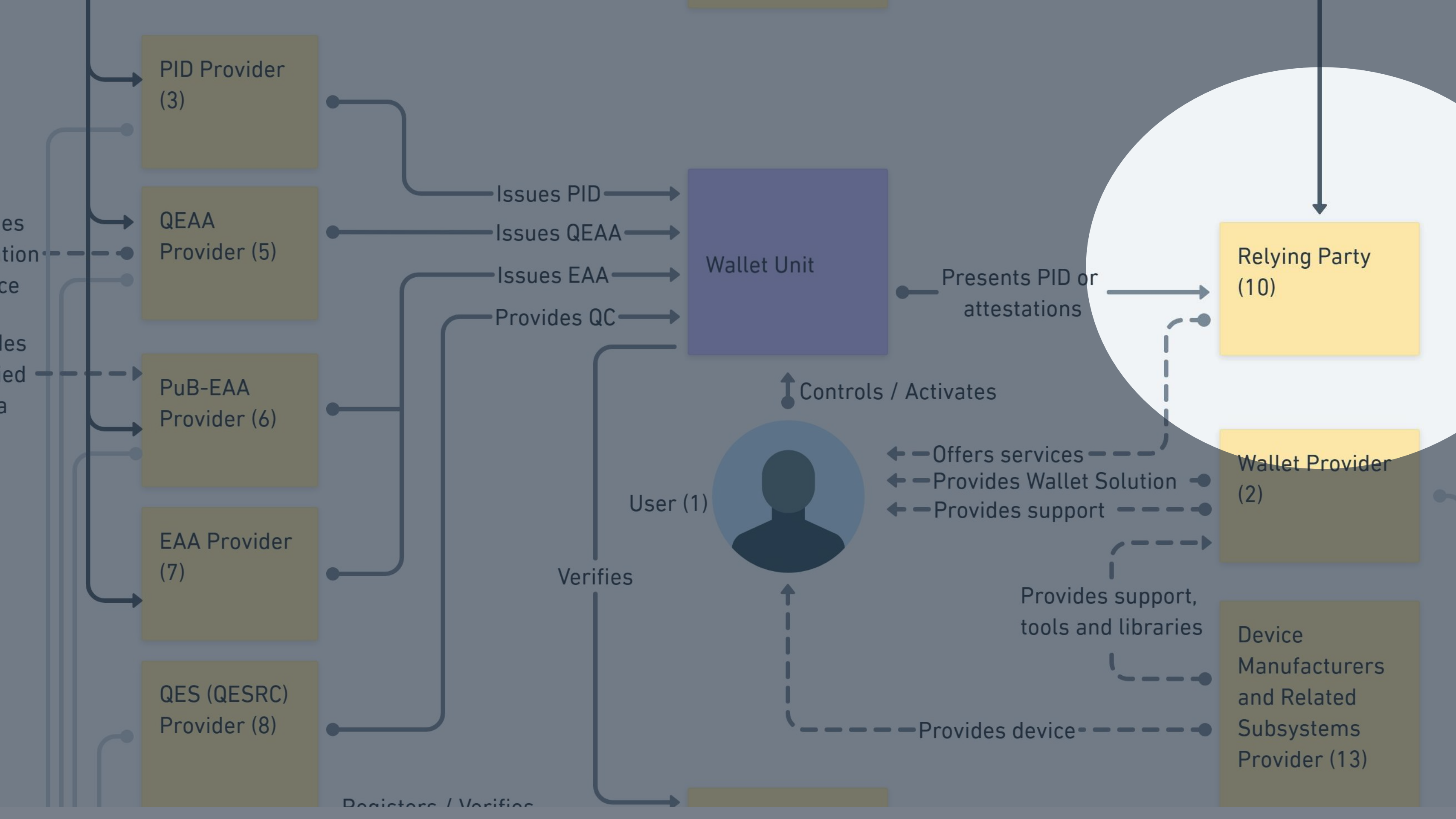


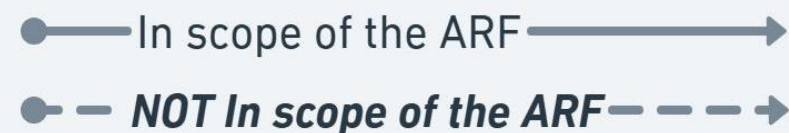












National
Accreditation
Body (15)

Conformity
Assessment
Body (11)

Supervisory
Body (12)

Attribute
Schema
Provider (14)

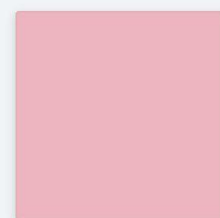
Legend



Primary Role



Component



Governance Role

Authentic
Source (9)

Provides
verification
service

Provides
qualified
data

PID Provider
(3)

QEAA
Provider (5)

PuB-EAA
Provider (6)

EAA Provider
(7)

QES (QESRC)
Provider (8)

Issues access certificate

Access
Certificate
Authority (16)

Issues access certificate

Issues PID

Issues QEAA

Issues EAA

Provides QC

Wallet Unit

Controls / Activates

User (1)

Verifies

Registers / Verifies

Trusted List
Provider (4)

Presents PID or
attestations

Relying Party
(10)

Offers services

Provides Wallet Solution

Provides support

Wallet Provider
(2)

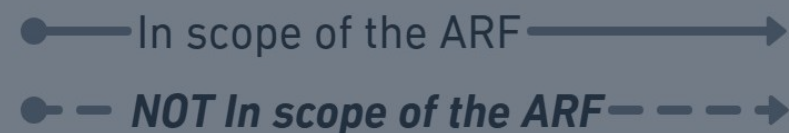
Provides support,
tools and libraries

Provides device

Device
Manufacturers
and Related
Subsystems
Provider (13)

Registers / Verifies

Provides support



National
Accreditation
Body (15)

Conformity
Assessment
Body (11)

Supervisory
Body (12)

Attribute
Schema
Provider (14)

Legend



Primary Role



Component



Governance Role

Authentic
Source (9)

Provides
verification
service

Provides
qualified
data

PID Provider
(3)

QEAA
Provider (5)

PuB-EAA
Provider (6)

EAA Provider
(7)

QES (QESRC)
Provider (8)

Issues access certificate

Registers / Verifies

Access
Certificate
Authority (16)

Wallet Unit

User (1)

Verifies

Trusted List
Provider (4)

Issues PID

Issues QEAA

Issues EAA

Provides QC

Controls / Activates

Offers services

Provides Wallet Solution

Provides support

Issues access certificate

Presents PID or
attestations

Provides support,
tools and libraries

Provides device

Registers / Verifies

Relying Party
(10)

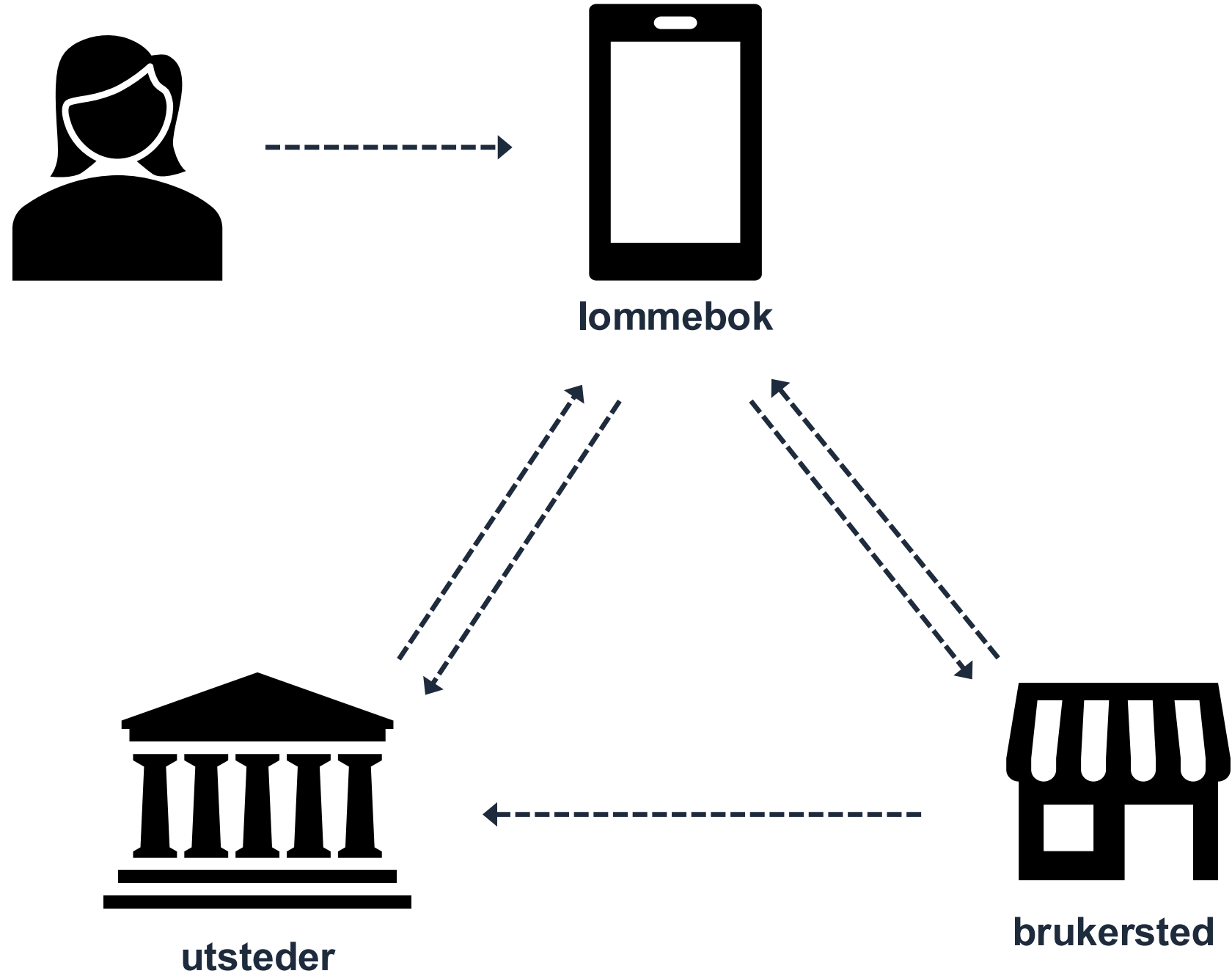
Wallet Provider
(2)

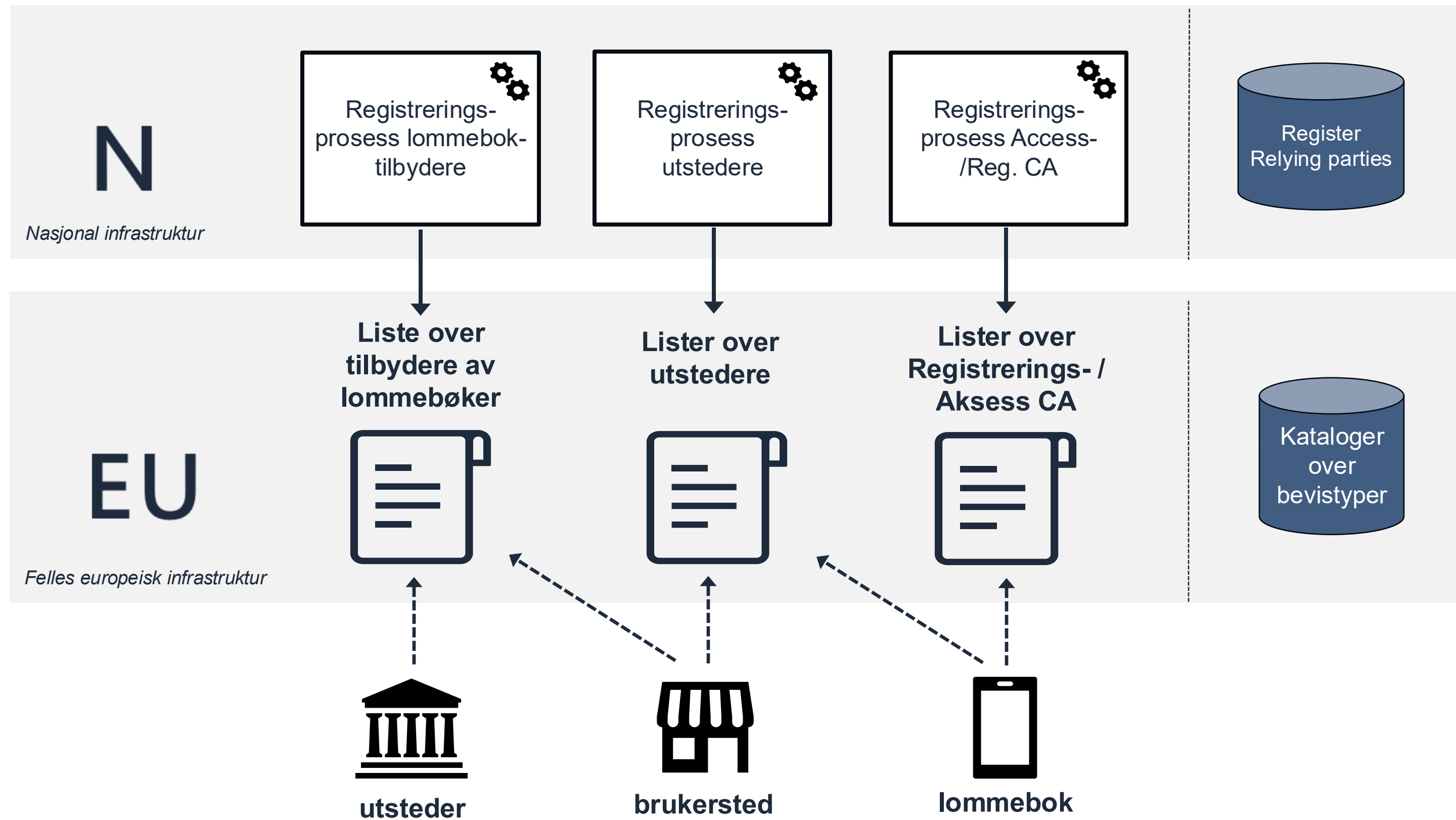
Device
Manufacturers
and Related
Subsystems
Provider (13)

Egenskapar me skal sjå på

- Økosystemet
- **Tillitsmodell**
- Lommeboka
- Bruke bevis
- Personvern

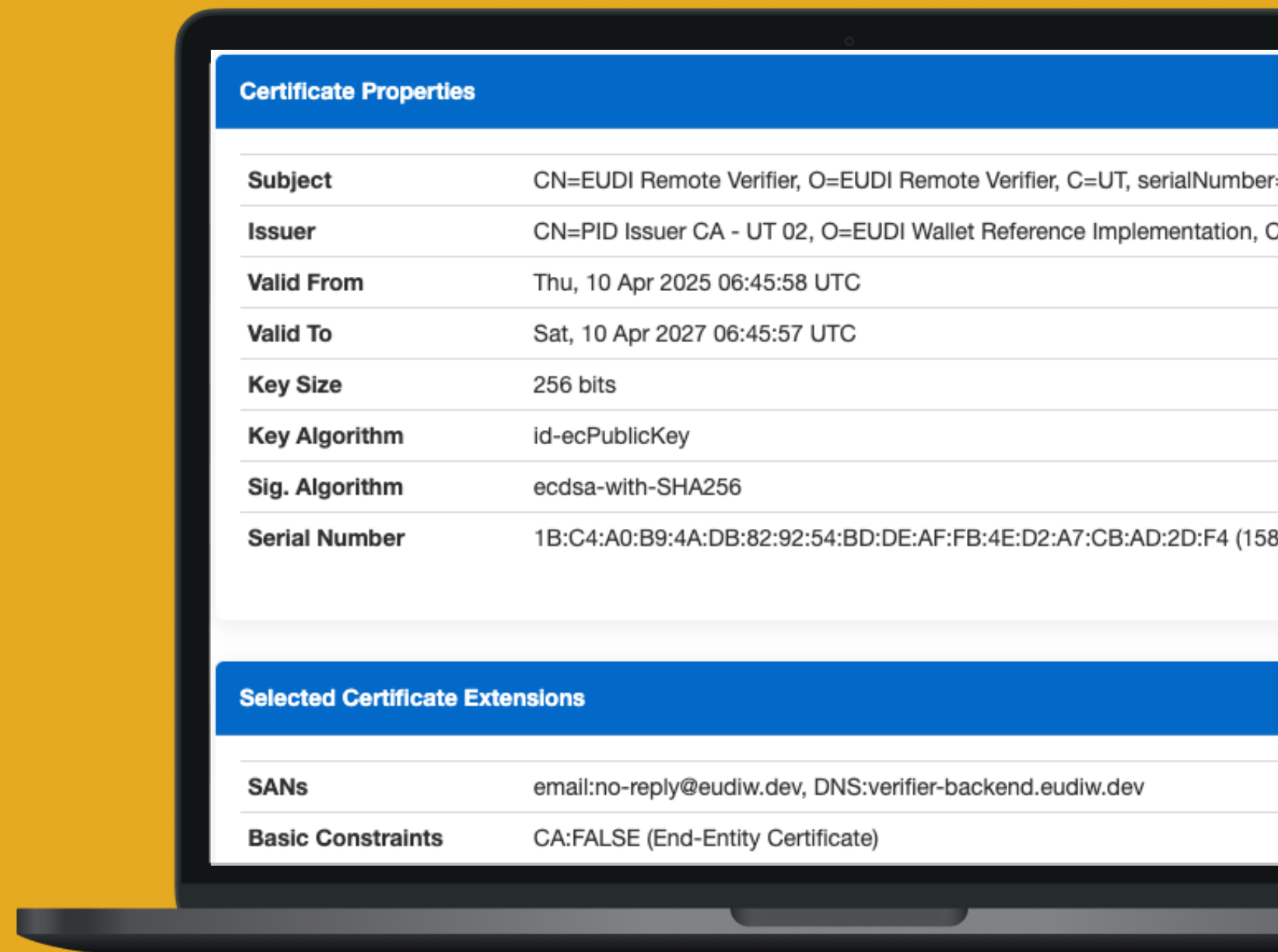






Aktørane treng 2 sertifikat

- Tilgangssertifikat (RPAC)
 - “RP access certificate” (X.509)
 - Autentisering - fortel kven du er
- Registreringssertifikat (RPRC)
 - “RP registration certificate” (JWT)
 - Autorisasjon:
 - kva data du har til hensikt å be om (eller utstede)
 - formålet med behandlinga

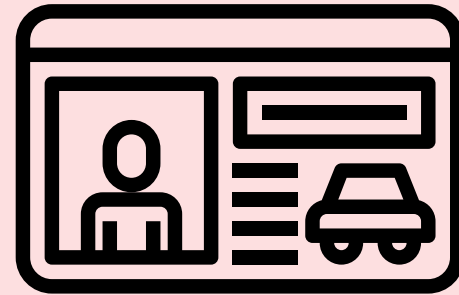


Bevis kan ha ulik styrkegrad



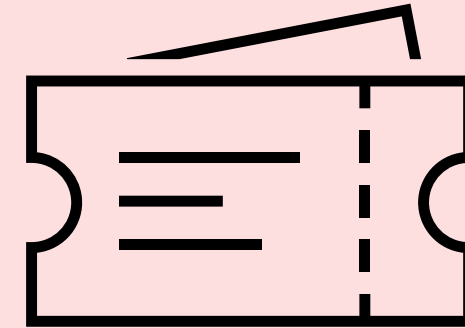
QEAA

Kvalifisert



Pub-EAA

“offentleg sektor”



EAA

“relativt uregulert”

Årleg sertifisering

Skal notifiserast

X.509 + Trustlist

Eingongssertifisering

Skal notifiserast

X.509 + Trustlist

Ingen krav til sertifisering

Frivillig registrering

Alternative tillitsrammeverk

Egenskapar me skal sjå på

- Økosystemet
- Tillitsmodell
- **Lommeboka og WSCD**
- Bruk av bevis
- Personvern



2009:



EUDIW

litt meir enn “just another app” ...

WSCD...what ?

WSCD - Wallet Secure Cryptographic Device

a tamper-resistant device that

[...]

protect critical assets

and

securely execute cryptographic functions.

Wallet Unit består av:

Sentralt:

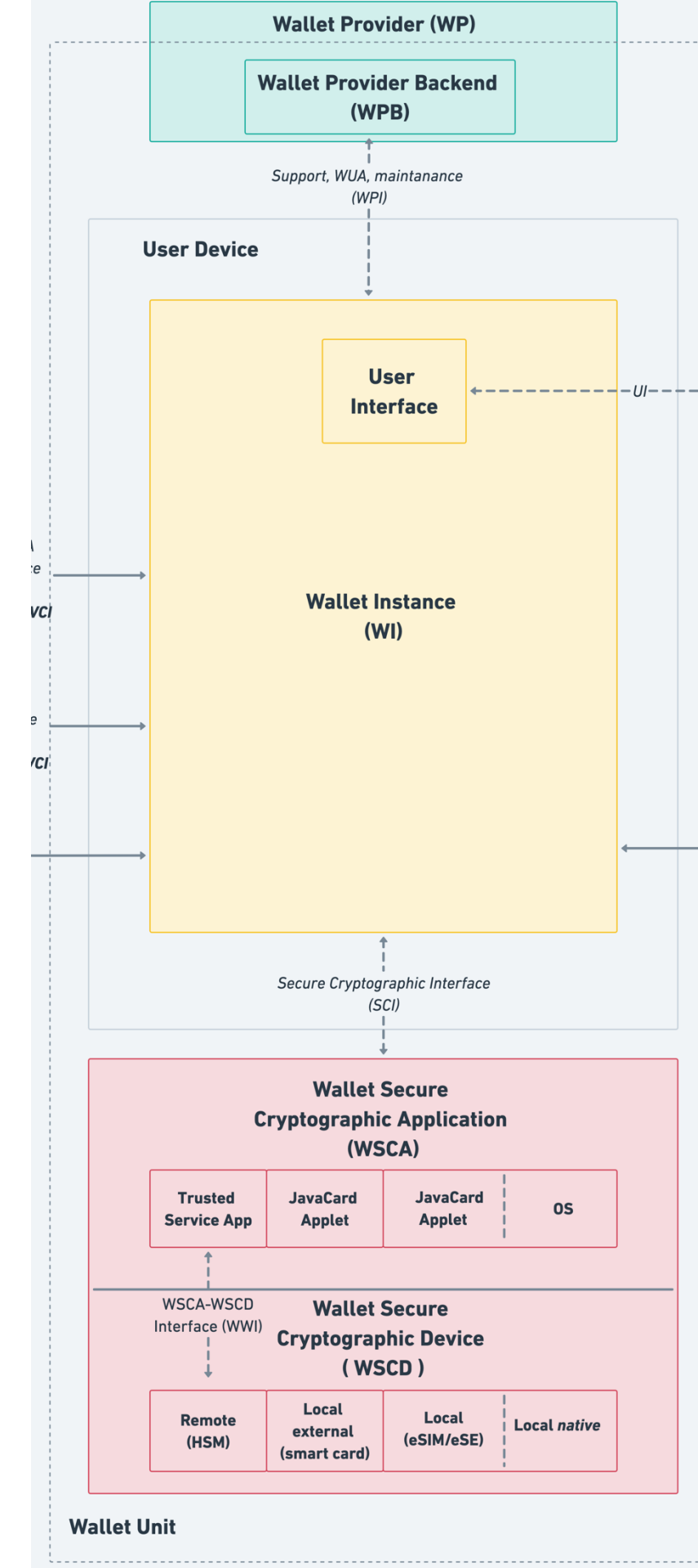
- **Wallet Provider Backend**

På brukaren sin device:

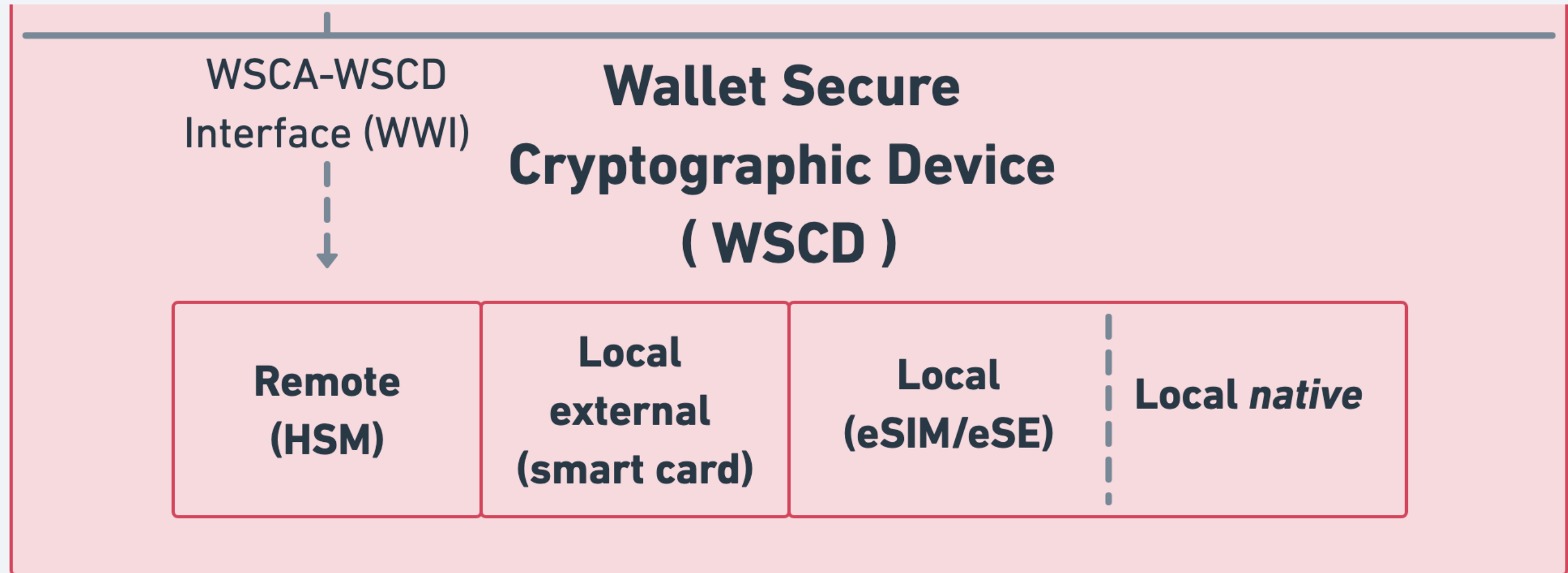
- **Wallet Instance**

Enten på brukaren sin device eller sentralt:

- **Wallet Secure Cryptographic Application**
- **Wallet Secure Cryptographic Device**



4 ulike teoretiske realiseringar av WSCD:



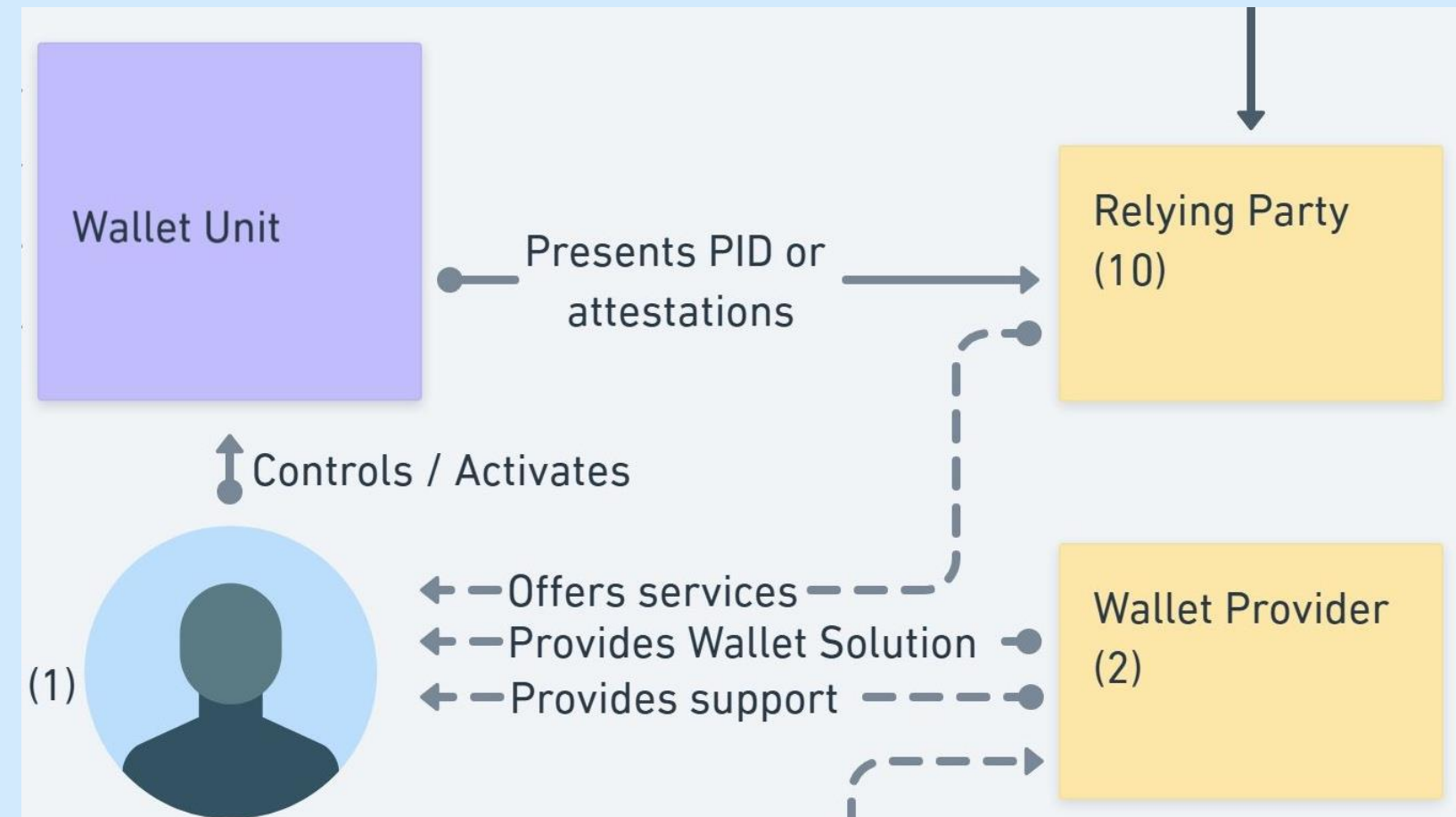
Egenskapar me skal sjå på

- Økosystemet
- Tillitsmodell
- Lommeboka
- **Bruke bevis**
- Personvern

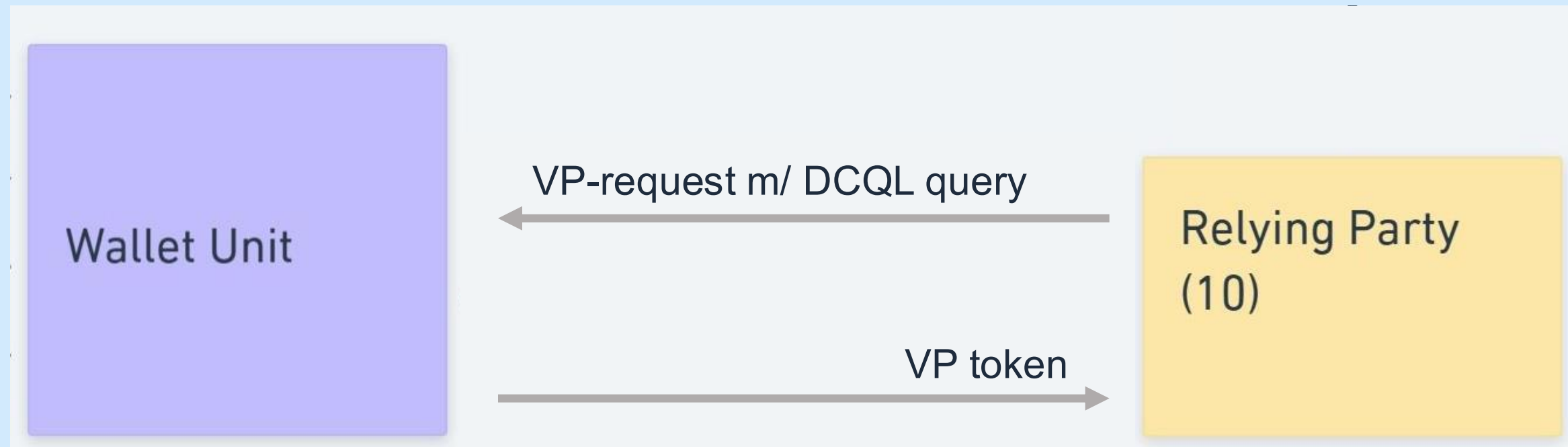


OpenID for Verifiable Presentation (OpenID4VP)

- Bygger på OAuth2
 - Kjent sikkerhetsmodell
 - Relativt enkel å implementere
- Breiare enn EUDIW
 - Format-agnostisk
 - Tillitsmodell-agnostisk



Bruke bevis – OpenID4VP (verifiable presentation)



Innhald i VP-request

```
{
  "x5c": [ "MIIDVDCCAvqgAwIBAgIJAlfxjT7NTwqKMAoGCCqG...",
  "typ": "oauth-authz-req+jwt",
  "alg": "ES256"
}.{

  // kva data treng eg ?
  "dcql_query": {

    "credentials": [
      { "id":  "førarkort",
        "format": "dc+sd-jwt",
        "meta": { "vct_values": ["org.iso.18013.5.1.mDL"] }
      }
    ]
  }
}
.
<signature value>
```

Innhold i VP-request

```
{
  "x5c": [ "MIIDVDCCAqAwIBAgIJAlfxjT7NTwqKMAoGCCqG...",
  "typ": "oauth-authz-req+jwt",
  "alg": "ES256"
}.{

  // kva data treng eg ?
  "dcql_query": {

    "credentials": [
      { "id":  "førarkort",
        "format": " dc+sd-jwt ",
        "meta": { "vct_value": "org.iso.18013.5.1.mDL" },

        "claims": [ {"path": ["org.iso.18013.5.1.mDL", "age_over_18"]}

      ]
    ]
  }
}
```

Innhold i VP-request

```
{
  "x5c": [ "MIIDVDCCA vqgAwIBAgIJAlfxjT7NTwqKMAoGCCqG...",
  "typ": "oauth-authz-req+jwt",
  "alg": "ES256"
}.{

// kva data treng eg ?
"dcql_query": {

  "credentials": [
    { "id":  "førarkort",
      "format": "dc+sd-jwt ",
      "meta": { "vct_value": "org.iso.18013.5.1.mDL" },

      "claims": [{"id": "gamal_nok", "path": ["org...mDL", "age_over_18"]}
                {"id": "fødselsdato", "path": ["org...mDL", "date_of_birth"]}],

      "claim_sets": [
        ["gamal_nok"],
        ["fødselsdato"]
      ]
    }
  ]
}
}
```

Innhold i VP-request

```
{  
  "x5c": [ "MIIDVDCCA vqgAwIBAgIJAlfxjT7NTwqKMAoGCCqG...",  
  "typ": "oauth-authz-req+jwt",  
  "alg": "ES256"  
}. {  
  
  "dcql_query": { ... }  
  
  // skal brukaren ta stilling til transksjonsspesifikke data?  
  "transaction_data": {  
  
    "type": "kiosksalg",  
    "vare": "1 pølse i brød",  
    "beløp": 45,  
  
    "credential_ids": [ "urn:no:mikrobetalingsbevis"],  
    "transaction_data_hashes_alg": "..."  
  }  
}
```

Autentisering av brukerstad

```
{  
  //brukarstaden sitt aksessertifikat  
  "x5c": [ "MIIDVDCCAvqgAwIBAgIJAlfxjT7NTwqKMAoGCCqG...",  
  "typ": "oauth-authorized-req+jwt",  
  "alg": "ES256"  
}.  
  
  // fortelje kven klienten (brukerstaden) er  
  "client_id": "x509_san_dns:demo-brukarstad.eidas2sandkasse.net",  
  
  //korleis skal responsen sendast tilbake til klienten  
  "response_mode": "direct_post.jwt"  
  "response_uri": "https://demo-brukerstad.eidas2sandkasse.net  
  
  "client_metadata": {  
    ...  
  }  
}
```

«Cross device»-flyt



eudi-openid4vp://demo-brukersted.test.eidas2sandkasse.net?
client_id=x509_san_dns:demo-brukersted.test.eidas2sandkasse.net
&request_uri=https://demo-brukersted.eidas2sandkasse.net/c7cd...f2a8

Request Object (RFC 9101)
Her "via reference" over GET

(kan også bruke POST, da kan wallet samstundes fortelle
Relying Party sine kapabiliteter)

Respons med vp_token

```
“vp_token”: { “førerkort”: [“eyJhGci...”] }
```



```
{
```

```
  "vct": "org.iso.18013.5.1.mDL",
```

```
  "age_over_18": true
```

```
  "iss": "https://issuer.vegvesen.no"
```

```
  "expiry_date": "2026—01-01"
```

```
  ...
```

```
  "cnf": { "jwk": { "kty": "EC", "crv": "P-256",  
    "x": "52aDI_ur05n1f_p3jiYGUU82oKZr3m4LsAErM536crQ",  
    "y": "ckhZ-KQ5aXNL91R8Eufg1aOf8Z5pZJnIvuCzNGfdnzo" } },
```

```
}
```

Autentisering = PID

```
{  
  "vct": "urn:eudi:pid:de:1",  
  
  "given_name": "Jean",  
  "family_name": "Dupont",  
  
  "birthdate": "1980-05-23",  
  
  "nationalities": ["FR"],  
  "place_of_birth": { "country": "NO" },  
  
  "issuing_country": "DE"  
}
```

Egenskapar me skal sjå på

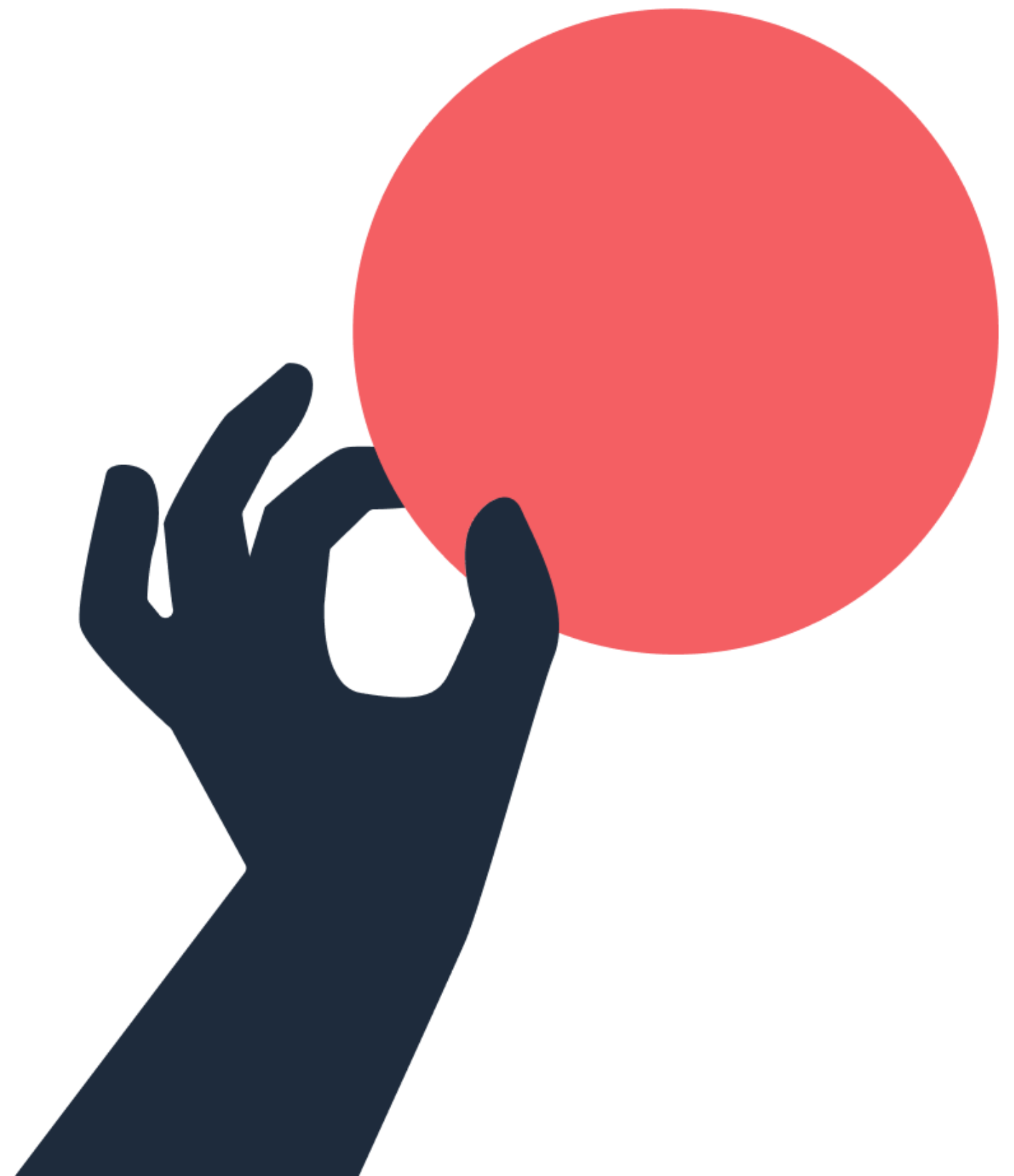
- Økosystemet
- Tillitsmodell
- App-arkitekturar
- Bruk av bevis
- **Personvern**



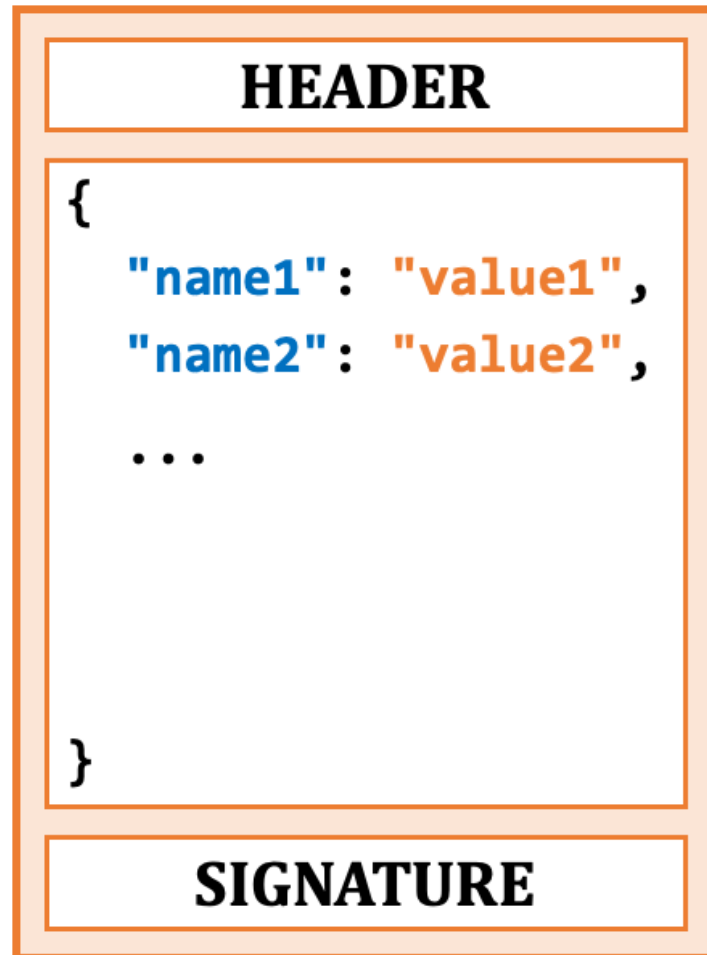
Selective disclosure

Korleis dele eit utdrag av eit signert bevis, og likevel validere signaturen?

- Hovudeigenskap ved Verifiable **Presentations**
- Primært ein teknisk mekanisme for **dataminimering hjå brukarstad**

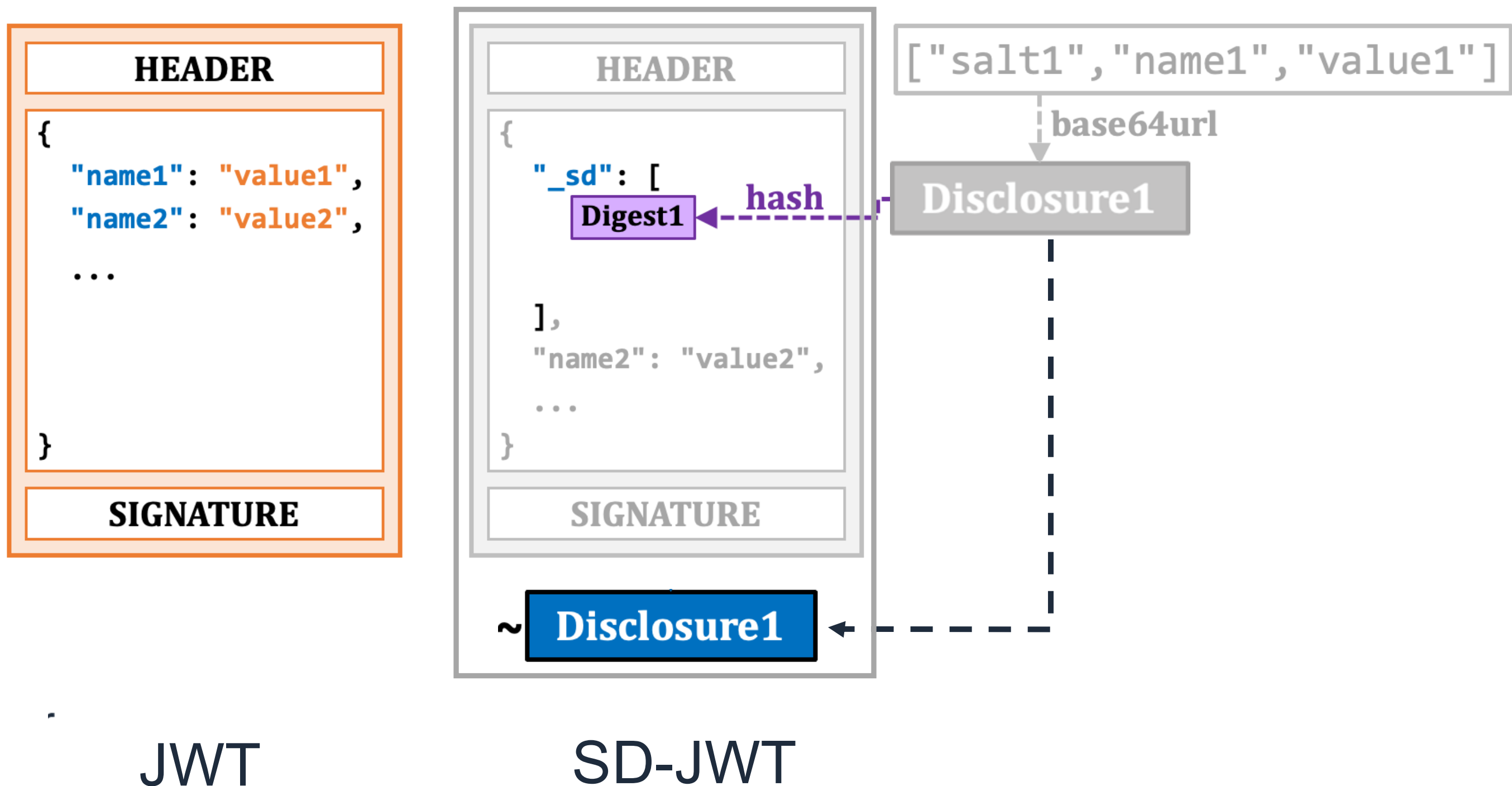


Selective disclosure med SD-JWT:

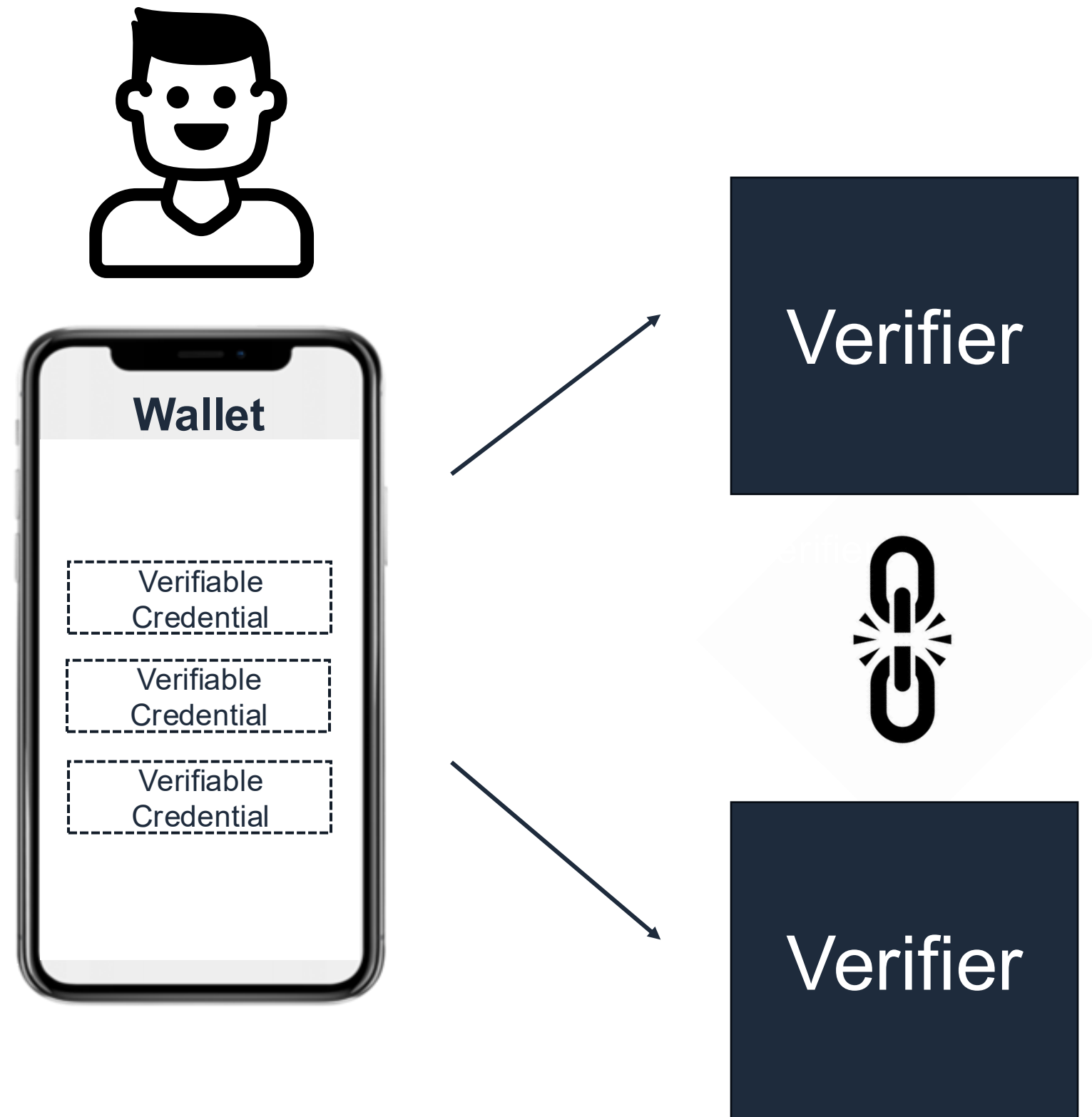


JWT

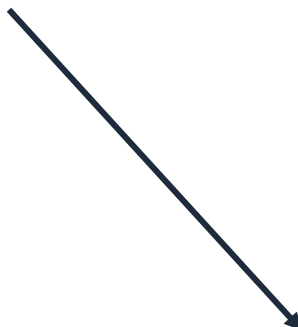
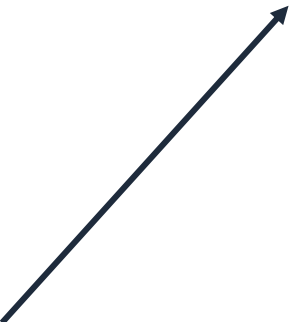
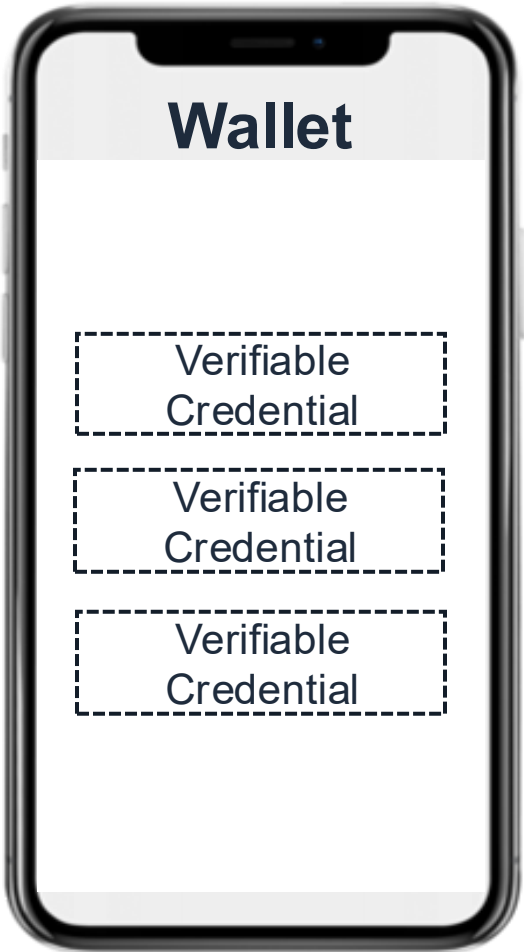
flytt attributtane på utsida av JWTen
...og erstatt med **digests** inni



**Unngå sporing
=unlinkability**



Unlinkability



Issuer

Verifier

Korleis kan sporing skje?

- Unike attributtar i sjølve bevisa (som fødselsnummer)
- Gjenbruk av statiske verdier, eller verdier som er avleda av statisk grunnlag, i sjølve protokollen:
 - hash'er
 - salt
 - nøkler
 - signaturer
 - WUA

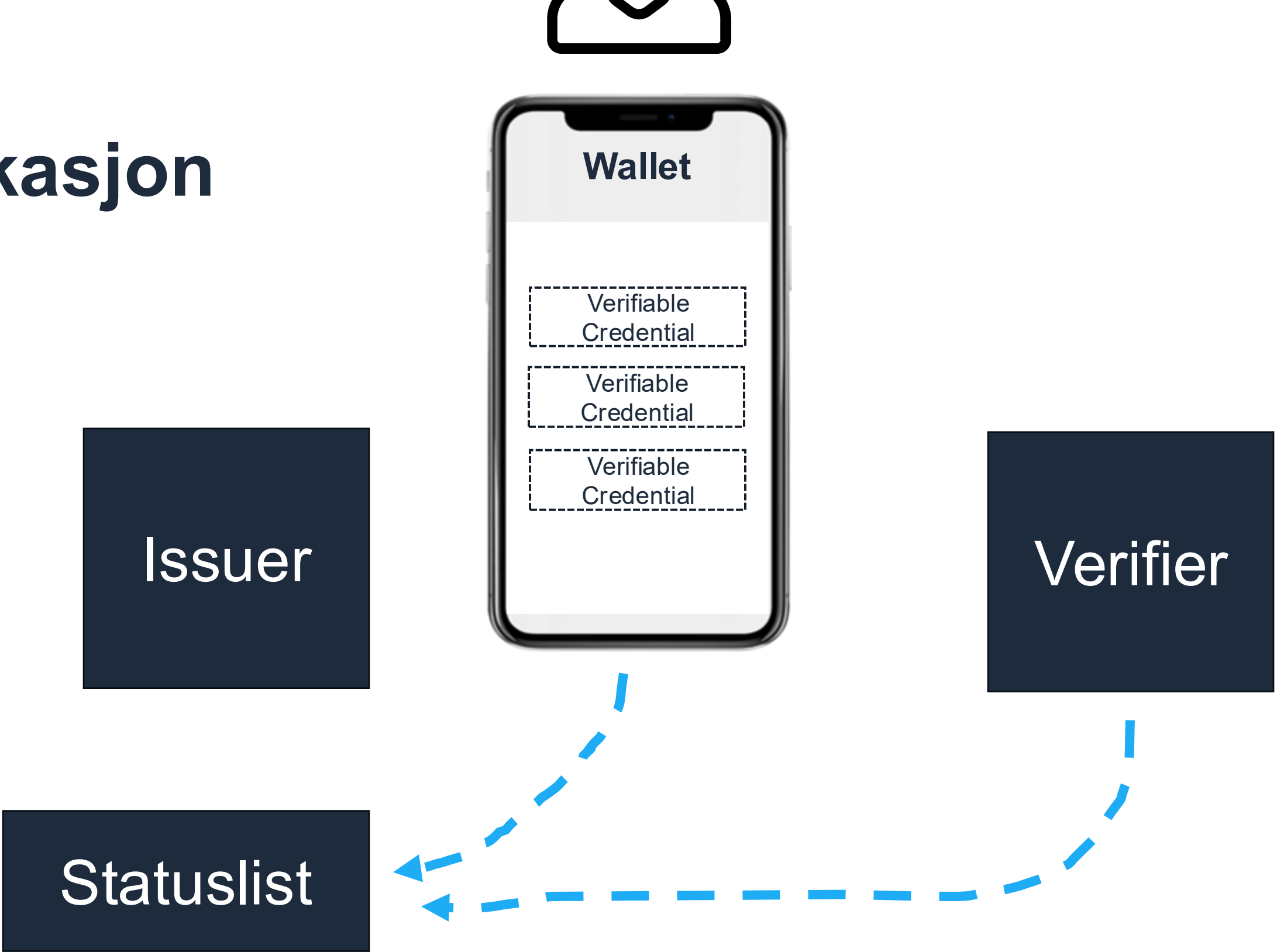


Korleis hindre sporing?

- **Batch issuance** av samme bevis
- **Kort bevis-levetid** og automatisert re-issuance
- Pseudonymisering med WebAuthn
- Zero-knowledge proof (ZKP)
- Hierarkiske nøklar



Revokasjon



Ny spec for **statuslister** sikrar unlinkablilty

- skal unngå at utstedar kan spore kven som bruker kva tenester

Inni eit enkelt-bevis:

```
"status": {  
  "status_list": {  
    "idx": 5  
    "uri": "https://example.com/statuslists/1",  
  }  
}
```

Felles statusliste:

```
"sub": "https://example.com/statuslists/1"  
"status_list": {  
  "bits": 1,  
  "lst": "H4sIAMo_jGQC_zvp8hMAZLRMLQMMAAAA"  
}
```

Deflate zlib

0x0 = VALID
0x1 = INVALID

1 0 0 1 0 1 0 0 0 1 0 0

Innsyn og transparens

- **Brukarstad-registra** gjev oversikt over kva data som organisasjonar **potensielt** kan samle inn om meg
- **Personleg dashboard** i lommeboka som viser din logg over “kva data har eg delt med kven, og når”



Demo



Digdir m/ venner
etablerer
nasjonal sandkasse
for digital lommebok



Sandkassen skal sikre at Norge er klar for lommeboka

- Utforske løsninger
- Bygge kompetanse og erfaring med digitale lommebøker
- Kunnskapsgrunnlag for nasjonale beslutninger

Hva er en sandkasse?

Sandkasser brukes ofte til å utvikle og teste løsninger for å utforske, teste og sikre at fungerer som de skal og er sikre før de tas i bruk. Dette bidrar til økt kvalitet og pålitelighet i digitale tjenester og systemer, samtidig som man minimerer risikoen for feil og problemer i produksjon.



Digdir tilbyr...

Kjernekomponenter

- Tillitsrammeverk
- Utstedar
- Demo-lommebok
- Arenaer for kunnskapsdeling

Du kan lage...

Det du vil!

- Utstedar
- Datakjelde
- Lommebok
- Brukarstad

Har du lyst til å delta?

Teknisk dokumentasjon:



<https://docs.digdir.no>

Ope diskusjonsfora:



Offentleg-PaaS:
#digdir-digital-lommebok

Privat sektor: bruk Slack Connect
<https://digdir-samarbeid.slack.com>



digdir.no

Digitaliseringsdirektoratet

postmottak@digdir.no

22 45 10 00

Postboks 1382 Vika, 0114 Oslo

Besøksadresser:

Industriveien 1, 8900 Brønnøysund

Skrivarevegen 2, 6863 Leikanger

Grev Wedels Plass 9, 0151 Oslo