OpenID Connect as a KYC Token distribution protocol

2018-09-28

Nat Sakimura(@_nat_en)

OpenID® Foundation

Chairman of the board

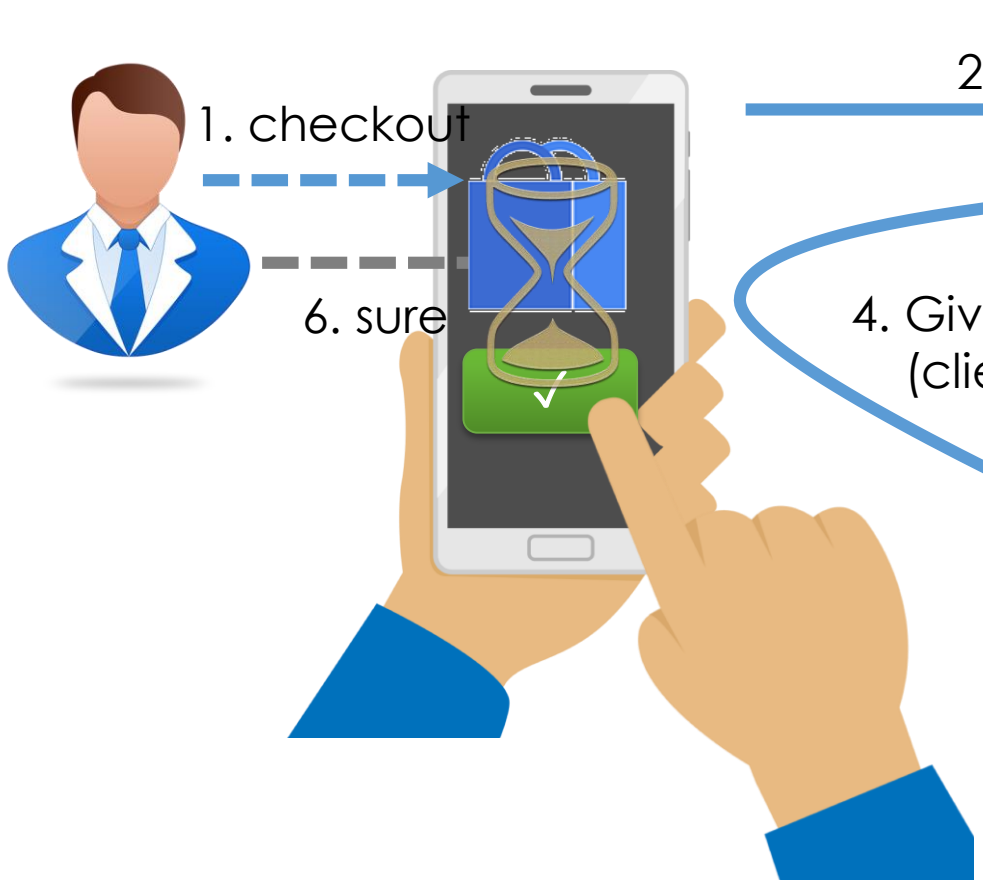
NRI 未来創発 Dream up the future.
野村総合研究所 Nomura Research Institute

Research Fellow

OAuth is the API protection mechanism of the choice now

It protects valuable resource (called Protected Resource) from unauthorized access using “access tokens”.

RFC6749 + RFC6750 defines the base spec.



2. checkout

OAuth Client

3. Create Authz Req
(client_id + scope)

4. Give me Authorization!
(client_id + scope + state)

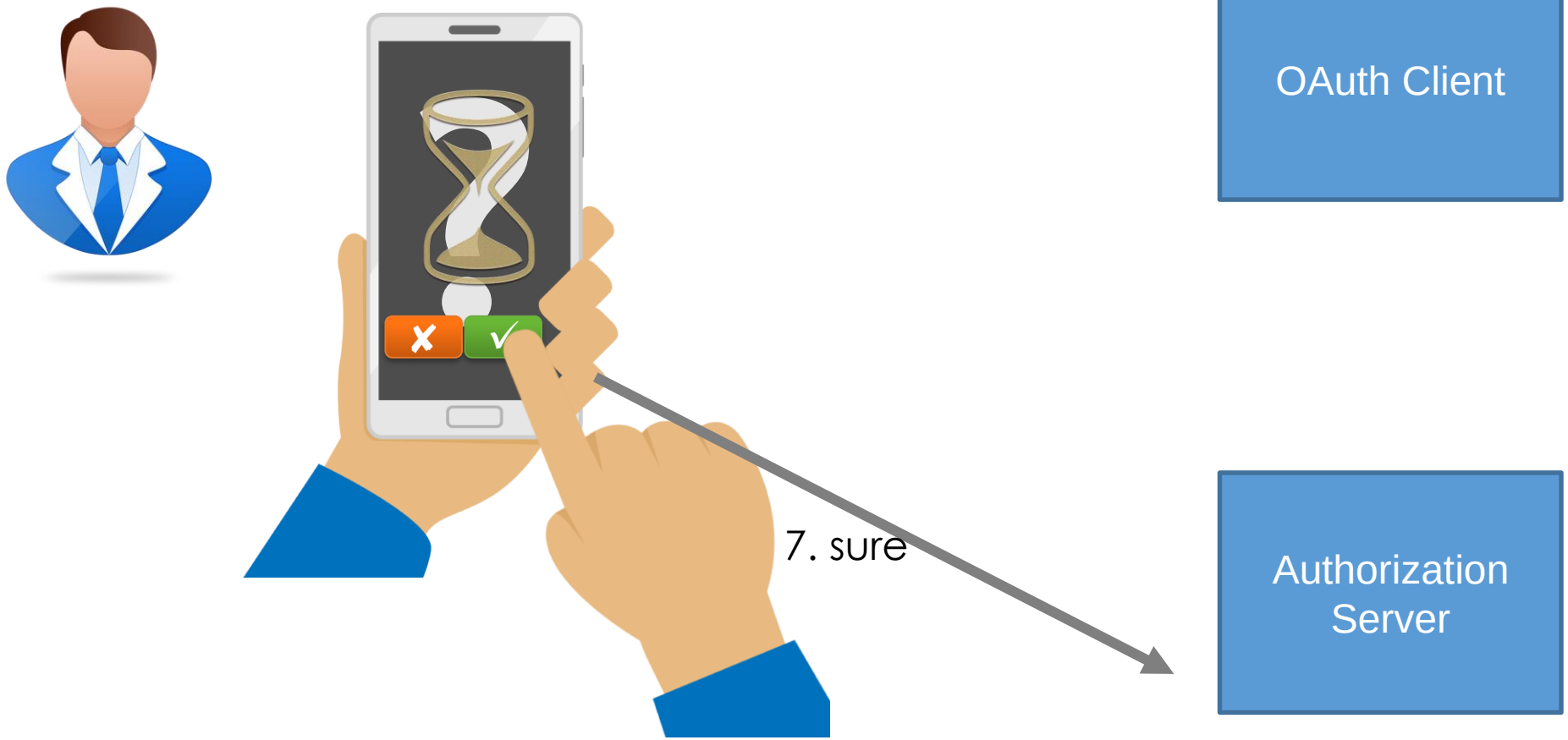
Authorization Server

8. Crate `code` that is bound to client_id

OAuth Client

5. Are you sure?

Authorization Server



9. Here is the Authorization!
(`code` + `state`)

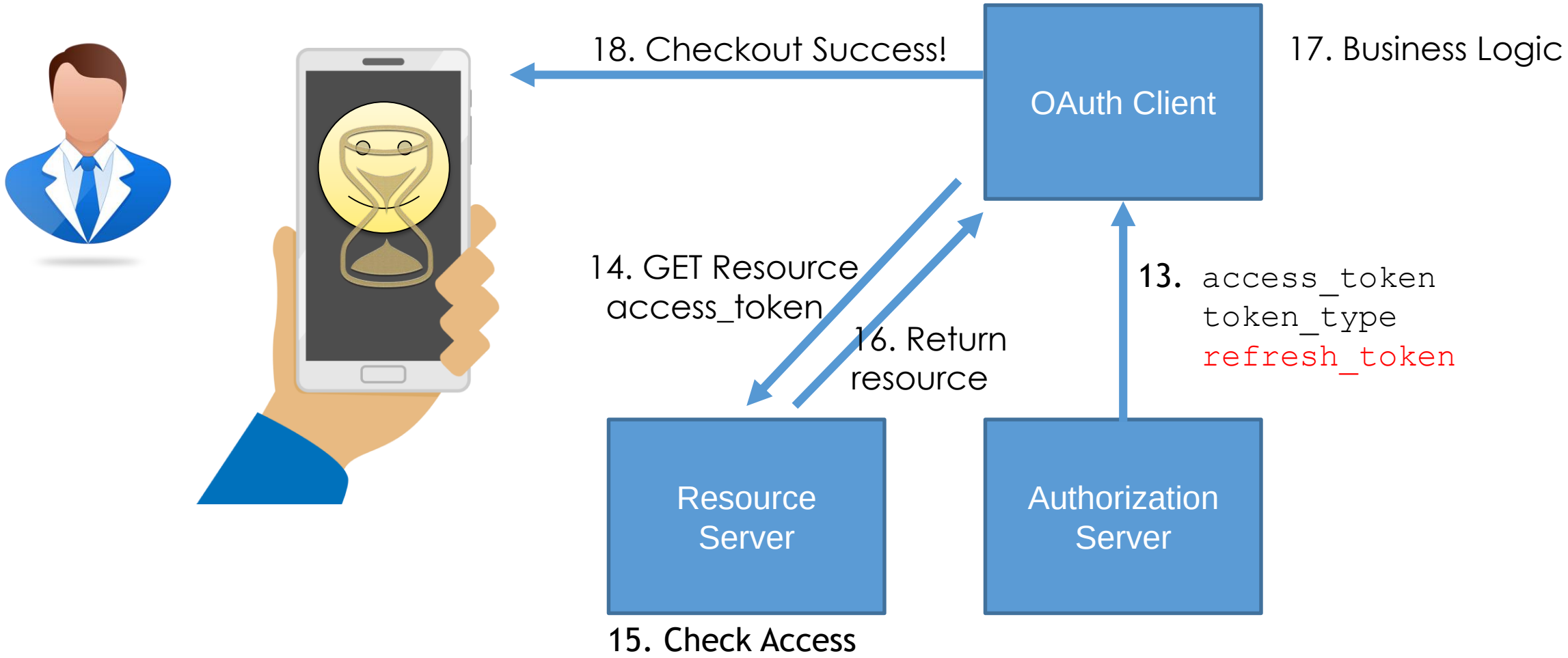
OAuth Client

10. Check `state`

11. Send
`code` +
`client_id` +
`client_secret`

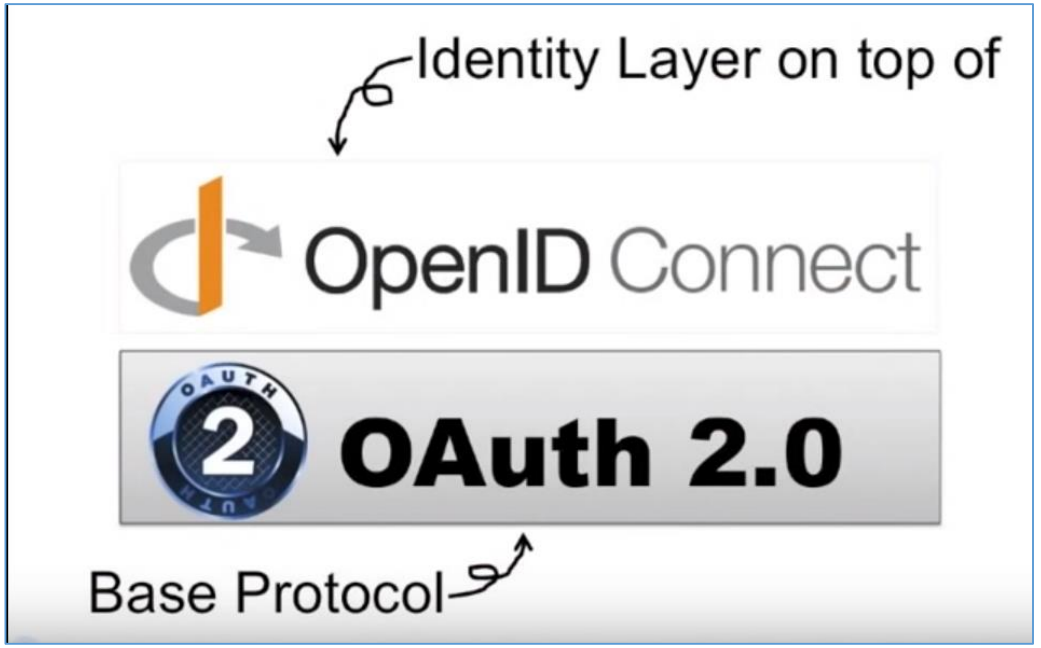
Authorization Server

12. Authenticate the client, check `code` is still valid and is bound to the `client_id`



OpenID Connect is the identity layer on top of OAuth.

- It defines
  - ID Token (Signed JSON Web Token with identity claims)
  - Protocols to request specific claims/attributes at a specific assurance level
  - Higher security mechanism
- Identity = set of attributes related to an entity (e.g., person, corporation, thing, process)
- JWT = JSON Web Token. RFC7519. The standard Token Format.
- JWT has three variants: JWS, JWE, JWS+JWE.
- JWS:= JSON Web Signature. JWT that is signed by the issuer's key.
- JWS is useful to store information as a signed token.
- E.g., Estonian Police.
- OIDC = OAuth + JWS+E(Identity)



(source) https://youtu.be/Kb56GzQ2pSk

It is the protocol of choice for federated authentication and identity federation

- As of April 2018, 92% of Azure Active Directory authentication happens over OpenID Connect.
- It is supported by mobile carriers (Mobile Connect)
- It is supported by many governments.
- UK OpenBanking's security profile is based on OpenID Financial-grade API Security Profile.

- Many vendors and open source products support it
  - List of certified implementations
  - https://openid.net/certification/

Requesting specific claim set or claims in OpenID Connect

- Method 1
  - Define a standardized OAuth scope, e.g. “kyc_token”
- Method 2
  - Ask for specific claims using claims parameter

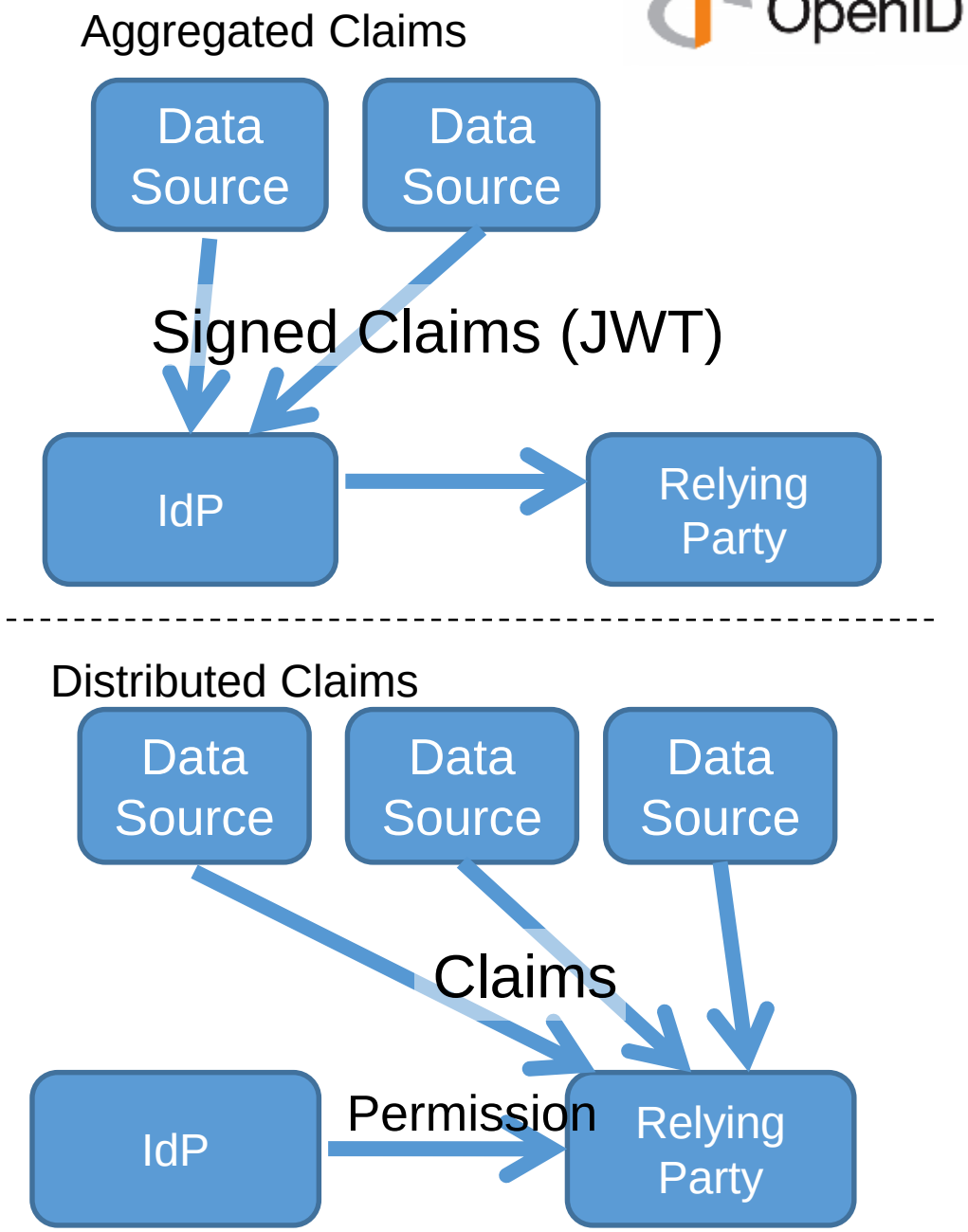
You can request a specific assurance level by using authentication context class reference.

- Use “acr” claim.
- Levels can be defined by a trust framework and should be registered to IANA acr registry.

```
{
  "userinfo":
   {
    "given_name": {"essential": true},
    "nickname": null,
    "email": {"essential": true},
    "email_verified": {"essential": true},
    "picture": null,
    “kyc_token”: header.payload.signature
   },
  "id_token":
   {
    "auth_time": {"essential": true},
    "acr": {"values": ["urn:mace:incommon:iap:silver"] }
   }
}
```

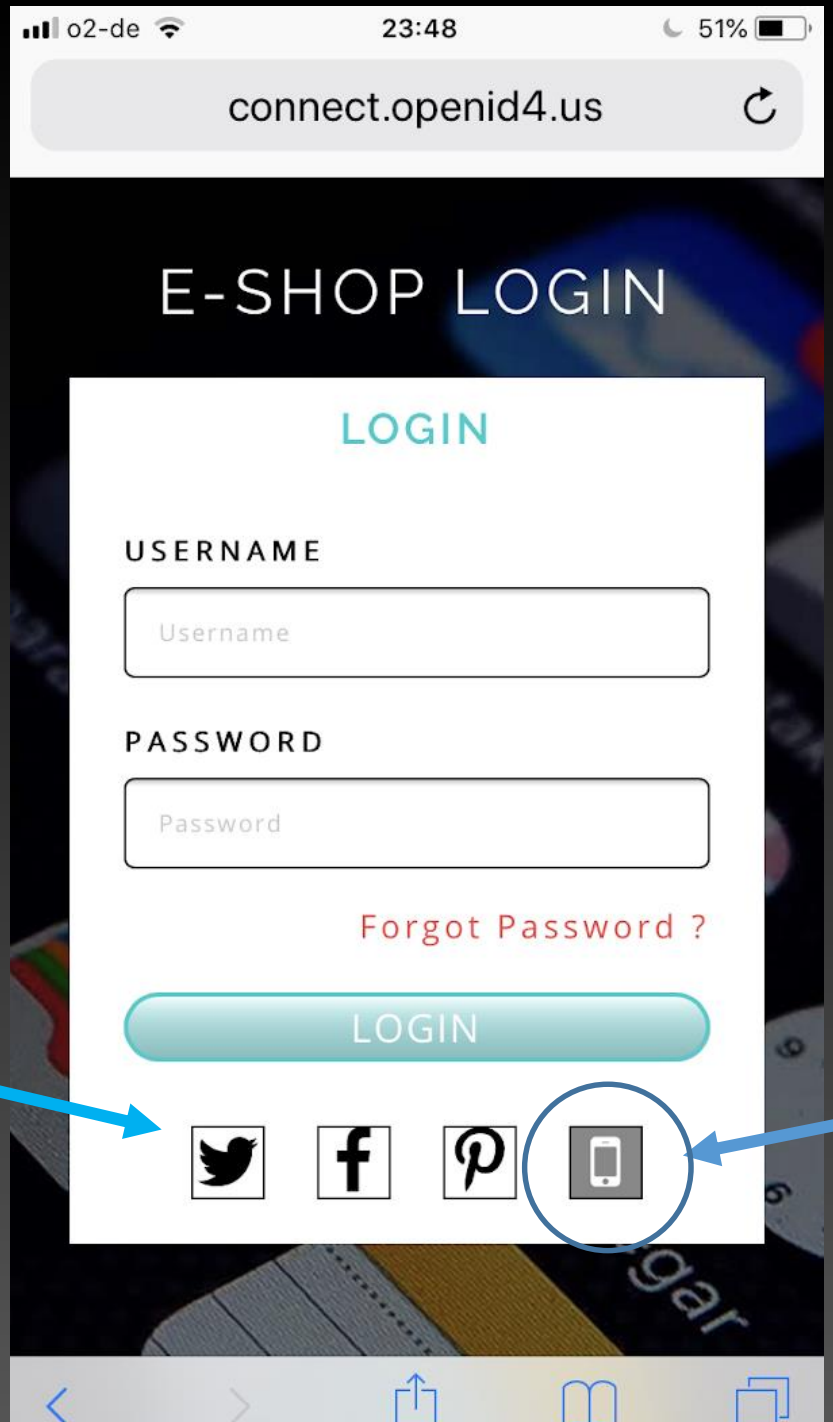
There are 4 ways to return the claims

- ID Token
  - Of the form: Header.Claims.Signature.
  - Each component is base64url encoded (ASCII Armored).
- Simple Claims
  - All the claims are provided by the IdP
- Aggregated Claims
  - Some claims are collected from the claims provider, esp. as a token.
- Distributed Claims
  - URL and relevant access tokens are returned to the client.
  - The client then can use them to retrieve claims from the claims provider directly.



If you are worried about user's account being taken away by the IdP or the "calling home" privacy problem, then you can use "Self-Issued OP"

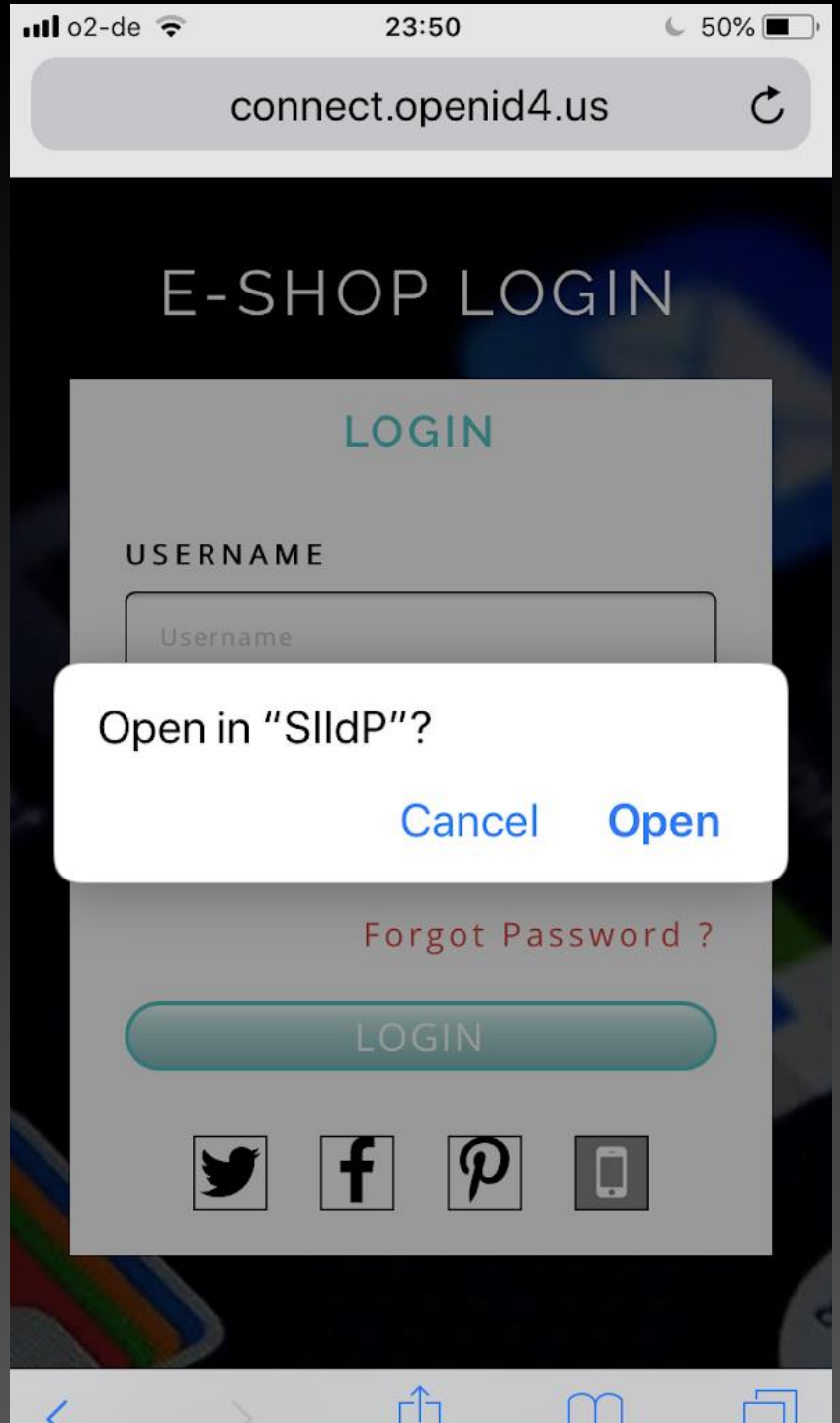
- In the self-issued OP, the IdP lives on your phone.
- User identifier is the hash of the generated signing key.
  - It can have any number of signing key to avoid correlation.
- Since it lives on the "localhost", DNS name is not needed.
  - Just the hash of the public key will do.
- By having the Self-issued OP provide the aggregated claims, the claim providers will become unable to find where they were provided.

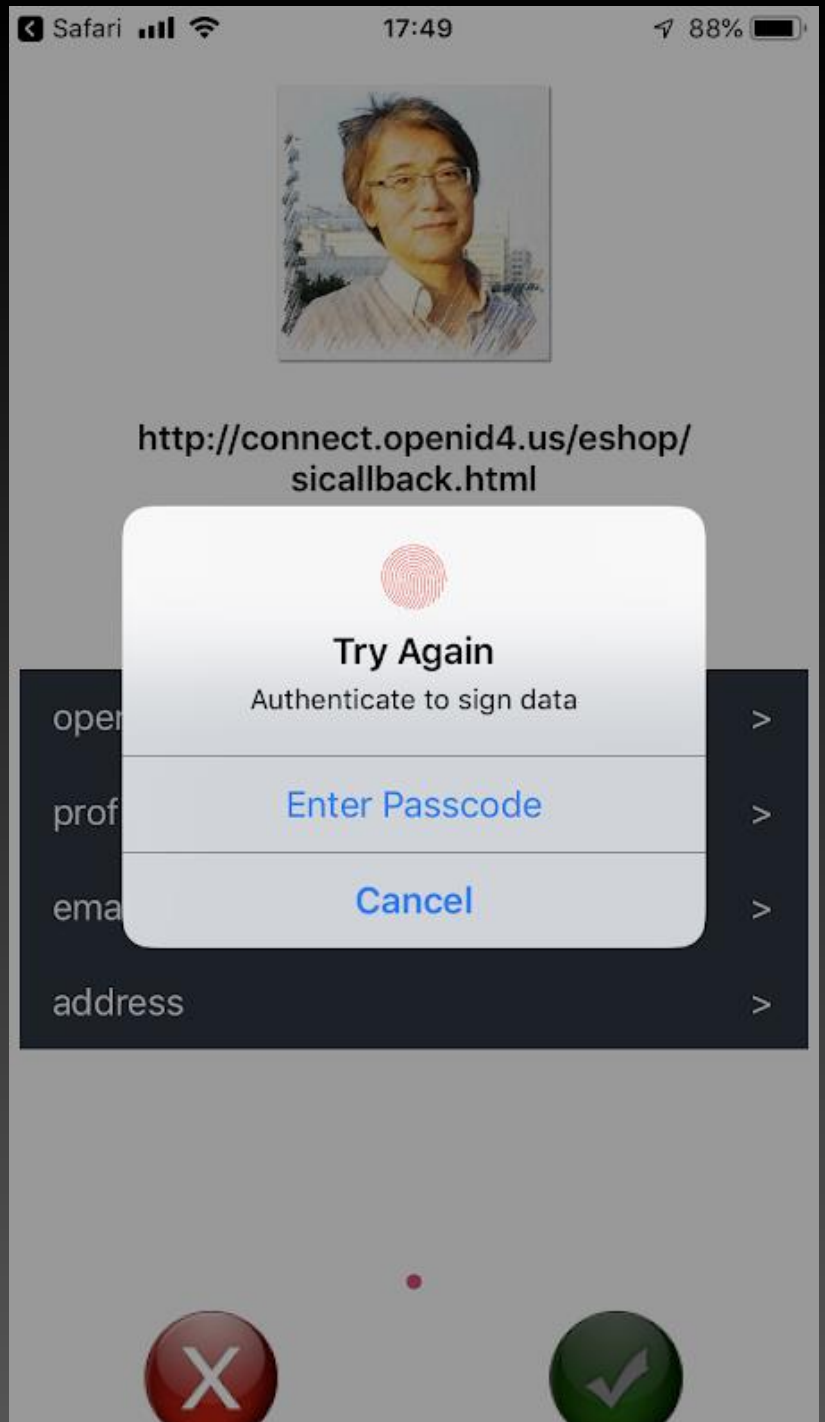


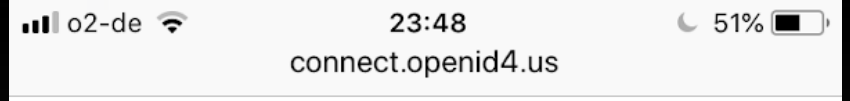
Social Logins

Self Issued Provider

Tap on it.


o2-de
23:50
50%
connect.openid4.us
E-SHOP LOGIN
LOGIN
USERNAME
Username
Open in “SIIdP”?
Cancel
Open
Forgot Password ?
LOGIN


Safari
17:49
88%
http://connect.openid4.us/eshop/
sicallback.html
Try Again
Authenticate to sign data
Enter Passcode
Cancel
oper
prof
ema
address



Hello vrv-X0e69uJD3jvFtAFKgn-tF1fmSqgJknN5v34AJkI


```
{
    "gender": "M",
    "iat": "2018-05-15T19:49:37.000Z",
    "family_name": "Sakimura ",
    "nonce": "12p29on",
    "sub": "vrv-X0e69uJD3jvFtAFKgn-tF1fmS
qgJknN5v34AJkI",
    "sub_jwk": {
        "kty": "RSA",
        "n": "AN8Yh9JyU1AnHpxO1TKsv6AEqlx
yxjHdH-ve1J3p-YfNVBw7az7zyAlftX_3l38OHGNa
hQ_fpysAUMIK8AAUp5f843BRm4i35d8mJBkGwNsPo
LpDY2aM6cYRrwTttBs4gaBLFI4wJo8r2jMRiLIrwp
yxPZEtwIyztlH1scDuU5orx8DR_lKffvEgA4iktRQ
3CUOVarYtoDoPRrls9OJxUxHSpqtTn7tezK0LKY6V
LrWB-cOD13XPsBPTsaJguyt1jvtrx1Gxsjs2MGktg
iYg-KqvTE0EsZAIxjVqdySWjtgqCOyLphXgyBdTC5
FyzxU9svNB4wyWVUYey6BrEmuFT50",
        "e": "AQAB"
    },
    "aud": "http://connect.openid4.us/esh
op/sicallback.html",
    "exp": "2018-05-15T19:54:37.000Z",
    "updated_at": 1526413732,
    "iss": "https://self-issued.me"
}
```