Introduction to OpenID Connect Core Ch.7 – Self Issued Identity Provider

2018-05-15

Nat Sakimura(@_nat_en)

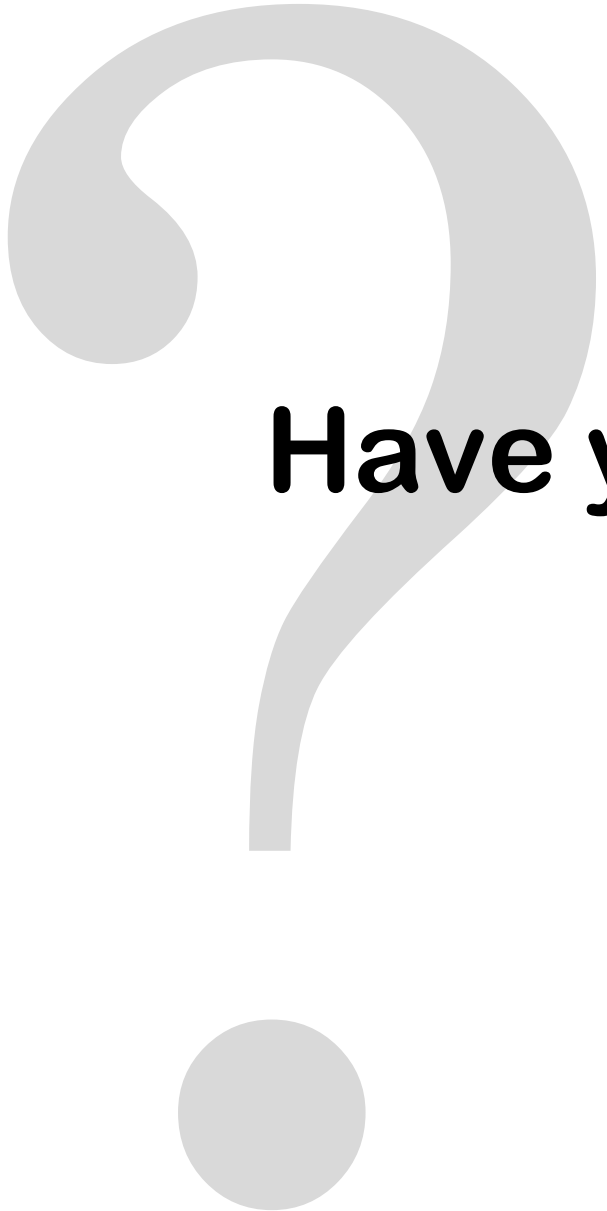
OpenID® Foundation

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

- OpenID® is a registered trademark of the OpenID Foundation.
- *Unless otherwise noted, all the photos and vector images are licensed by GraphicStocks.

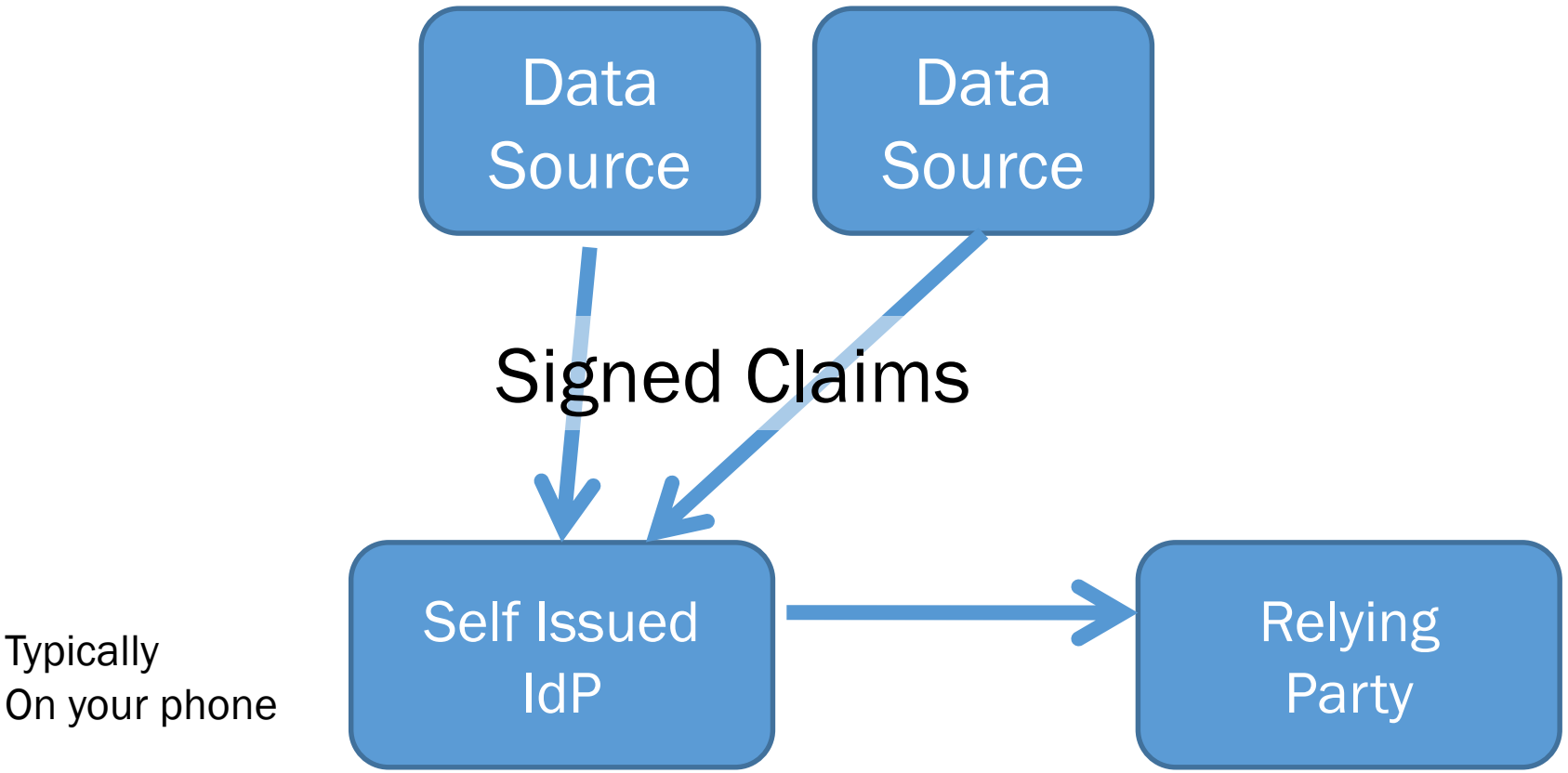


Have you read the Chapter 7 of OpenID Connect?

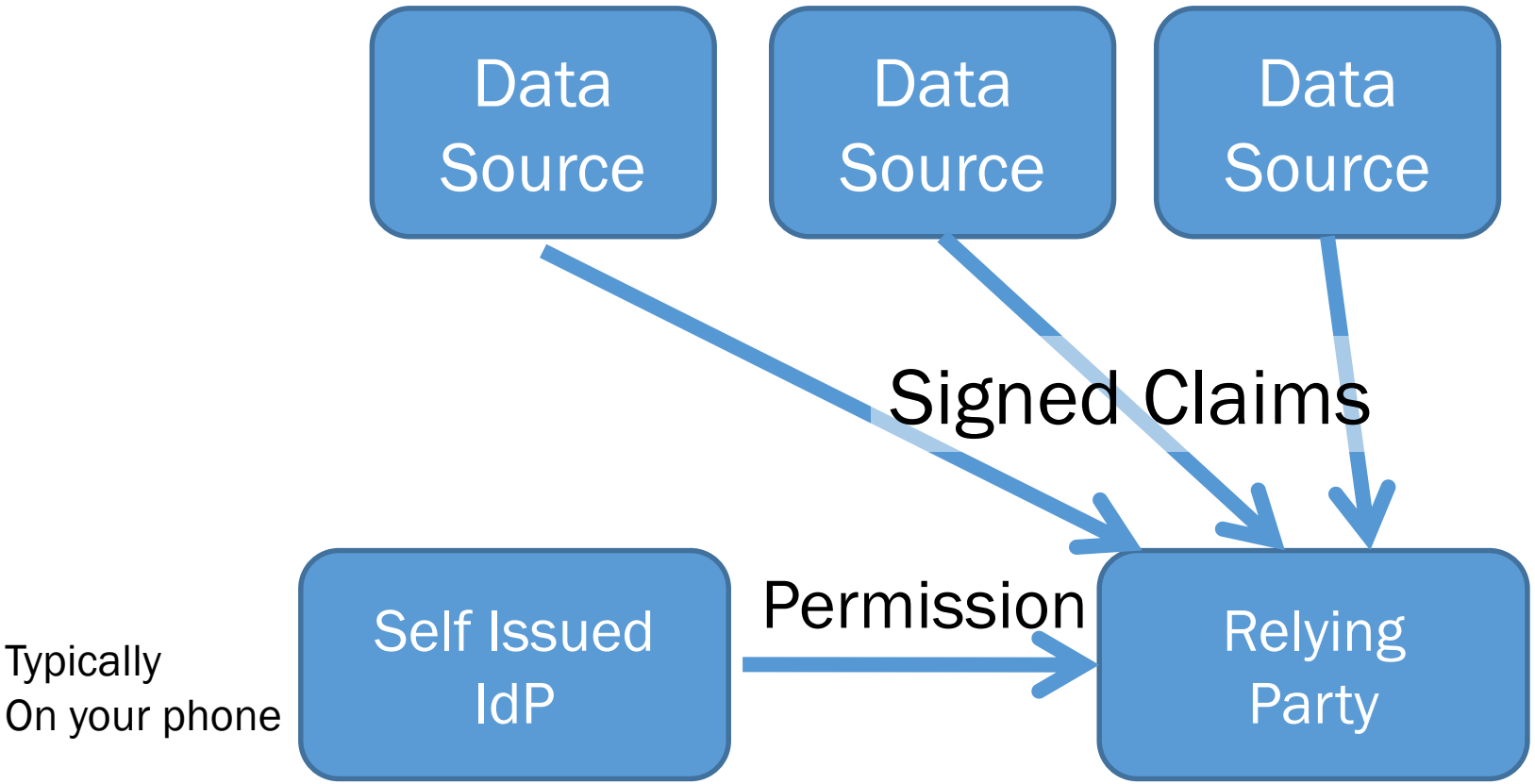
It is an IdP on your local machine

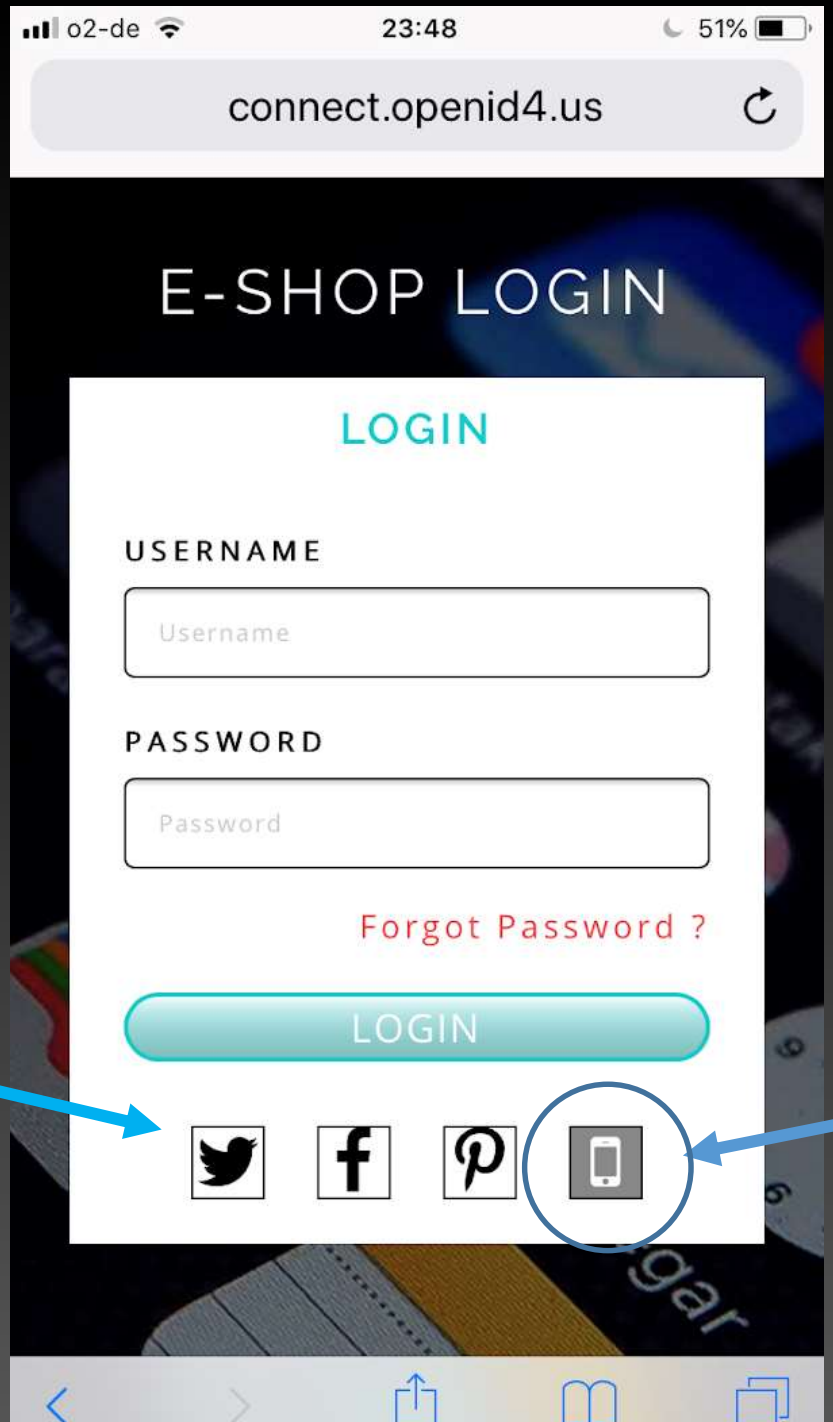
- I am the issuer of my “identity” therefor it will not be taken away
- Sounds a lot like “Self Sovereign Identity”, is it not?
- It does not need Blockchain, and does not leak information like current proposals that uses Blockchain.
- Wire-protocol-wise, it is OpenID Connect with a little twist.
- It can obviously use the platform supported Authenticator,
  - e.g. FIDO/WebAuthen supporting TEE through biometric unlocking.

Aggregated Claims



Distributed Claims



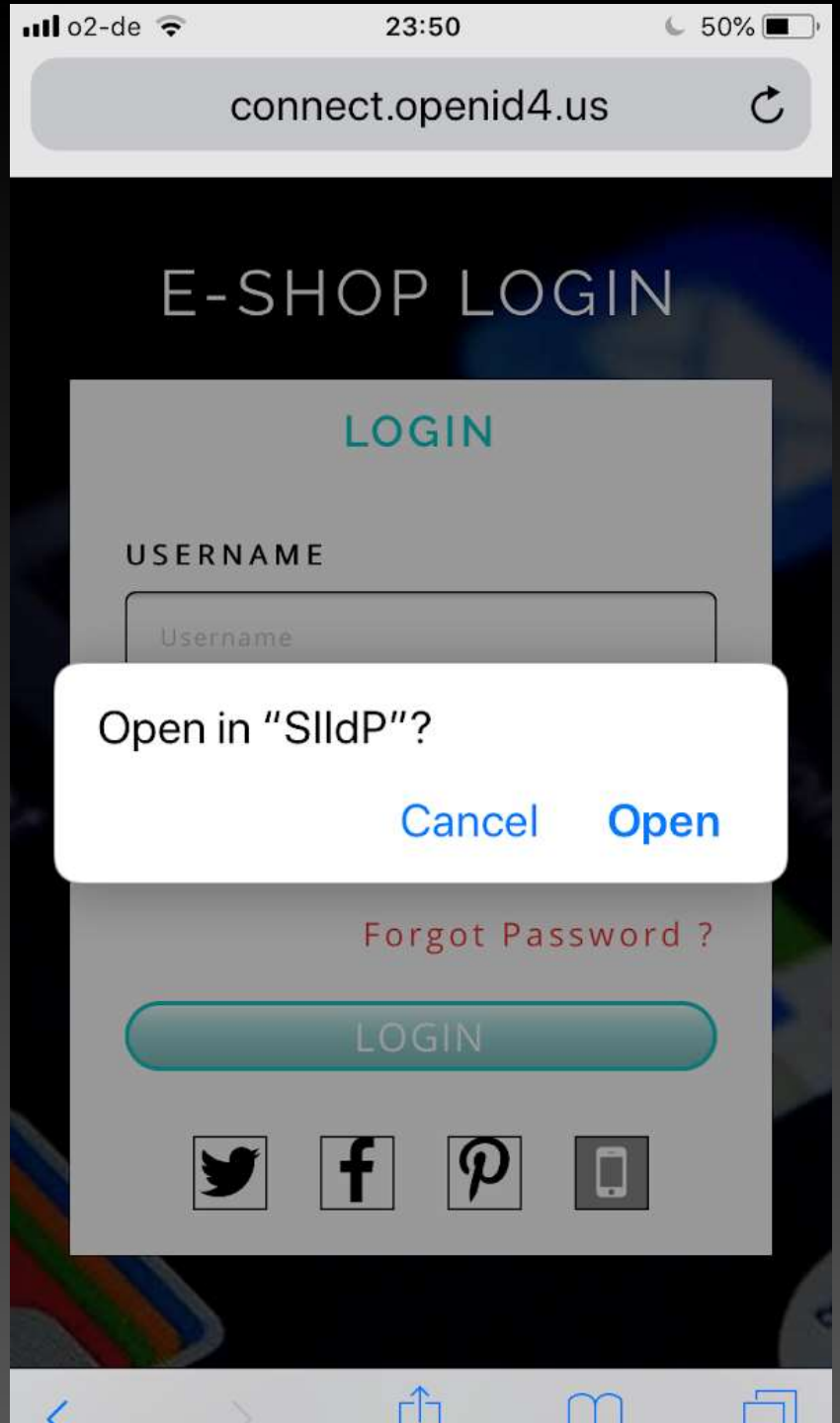


Social Logins

When Self Issued IdP is Supported by the client/RP, The RP should show an icon For it, e.g., a phone icon.

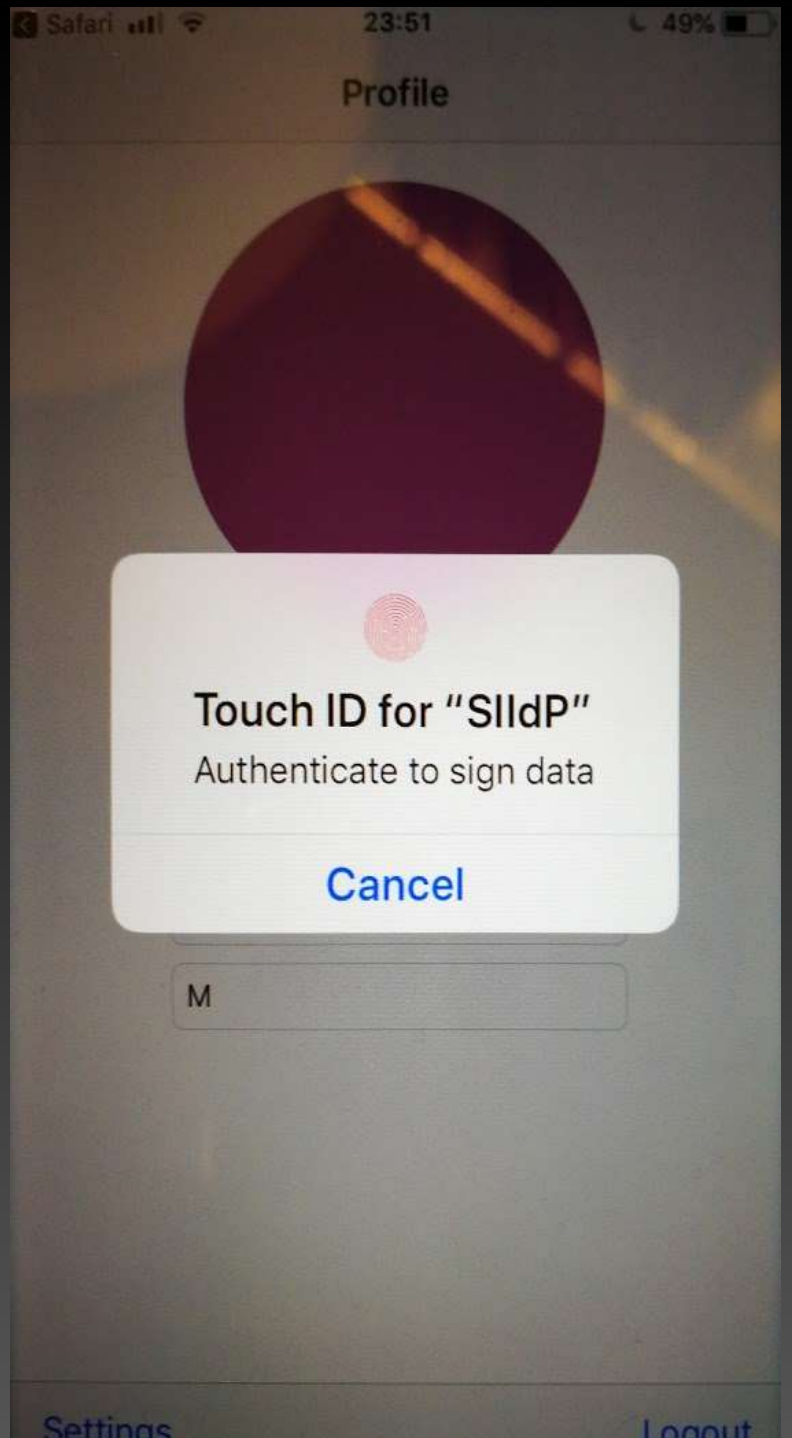
Self Issued Provider

Tap on it.



Since it is using Custom Scheme, I get asked if I want to open it.

Tap Open.



Use touch ID to unlock the private key in the keychain.

On Android, we can utilize TEE (Trusted Execution Environment).

And, you get a regular ID Token, which when decoded will be as on the right.

Hash of the public key that Belongs to the subject

Public key that belongs to the subject