**Use External Identity Providers for User Authentication**

**Status**

Proposed

**Context**

* Ease of implementation
* Increase useability because users do not need to remember more passwords
* Validating against existing trusted user repository

**Decision**

The proposed system would use Google, Facebook and Apple Identity provider services. The client applications would securely persist retrieved auth codes in the client. The API calls would authenticates using the retrieved access token from these identity providers.

The OAuth delegated protocol would be used for this authentication process.

Timeline

Description automatically generated

Architecture characteristics that required:

* Security
* Availability
* Accessibility
* Resilience
* Scalability
* Elasticity

Alternatives :

1. Use other Identity service providers such as

* WSO2
* OneLogin
* Centrify

1. Build in-house federated Identity provider

**Consequences**

Architecture tradeoff analysis

* The entire system would depend on 3rd party identity providers
  + This would cut down efforts of building own identity services and functionality
  + Proposed identity providers are reliable, renown and used by many other similar systems
* The scalability, security and user data storages are maintained by the service providers them self.
  + Compliances can be obtained using service provider’s compliances

Architecture fitness function

* Successfully authenticate all registered users against 3rd party Identity service provider