**Idea:** Create a authentication and authorization solution that could replace AD and can be used for SSO for on-premise and Cloud applications

**Expansion:** The solution is called a IDaas (Identity as a Service) with more or less the same features Balli expects. The prime players in the market are Ping, Centrify, Firebase, Azure AD.

All have an on-premise as well as a cloud offering for the product, have the ability to migrate existing ADs to the cloud or keep in sync the on-premise to the cloud along with plugin functionality to implement authentication/SSO for desktop and cloud apps. The only downside for enterprise acceptance is the cost and security in the cloud.

**Idea prerequisite:** IDaaS is an older concept and not much popular among enterprise customers and unlikely to be seen with SMBs or governmental institutions. One of the main reasons suspected for this lack of adoption is the security. Some enterprises are bound by laws when sharing data or physical location of data due to country laws, others are more concerned about the likelihood of a breach. For this idea to take shape we at least need the below in our product to retain a competitive edge

* Free or One-time payment option
* Serviceability and migration of existing ADs (probably MS AD)
* Pluggable architecture with all basic AD features
* Ability to provide an on-premise solution that can be hosted on some third party vendor like Azure or AWS or private cloud and managed by us.
* Scaling up/across, updates, offline access.
* Integration with Open-Id providers

**What we need**:

1. Need to develop the idea with some potential USP
   1. Agree on a end goal
   2. Agree on scope of what market we’ll be fighting for
2. Security Expertise
3. Niche selling point - (Free/Better migration/Marketing buzz/SSO)

Scenario 1 :

If any developer is working on any project as a freelancer or for company. If he has to write a module for authentication and authorization then he can either use our package or he can fork out our codebase from GitHub and use.

Scenario 2- for Small Company if they are working on more than one app and they want to do centrally managed authentication and authorization they can use this module as a different app where all authentication and authorization will be configured and rest all application can use this.

Scenario 3- we will host the same platform as software as service and onboard client and application and provide application services.

Module

1. Rest Based API for every operation
2. Angular UI for Configuring role for app or for organization
3. UI for Managing Permission for role.
4. UI for Manage User for app or organization
5. Audit log of every things.
6. RBAC is also used in app
7. Report for various activity for users and login.
8. IP Details of login
9. Handle DOS/DDOS
10. Security at Rest
11. Two factor authentication
12. Integration send grid
13. Integrate SMS Gateway
14. Sample Integration module for Java/PHP/VC++/C# etc

DB Design will be in My SQL and MS SQL also.

API will be developed in Asp.net Web API, Java, PHP considering most of our target users.

UI will be in Angular and Typescript.