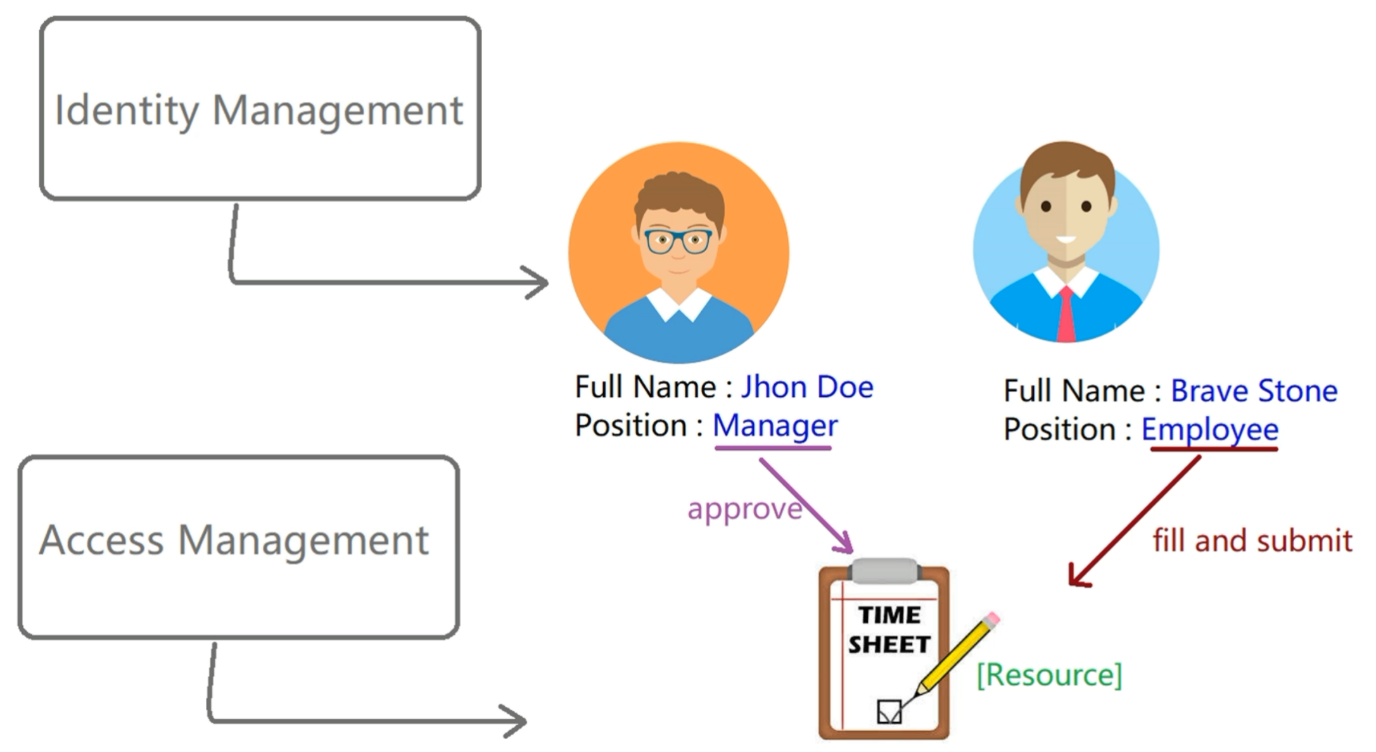
**IAM [Identity and Access Management]**

* Identity Management deals with:
  + Creating or onboarding identities into organization.
  + Managing user’s digital identities and its life cycle.
  + To provide right access to the right person.
  + In Identity Management Attributes are loaded to an Identity and those are managed throughout the life cycle of user.
* Access Management deals with:
  + Attribute which are loaded while Identity Management, now based on the value of these attributes, we take decisions in to allow or block that user from accessing that resource.



**5 Pillars of ForgeRock**

1. ForgeRock Access Management
2. ForgeRock Identity Management
3. ForgeRock Directory Services
4. ForgeRock Identity Gateway
5. Open ICF

**Basics of Access Management**

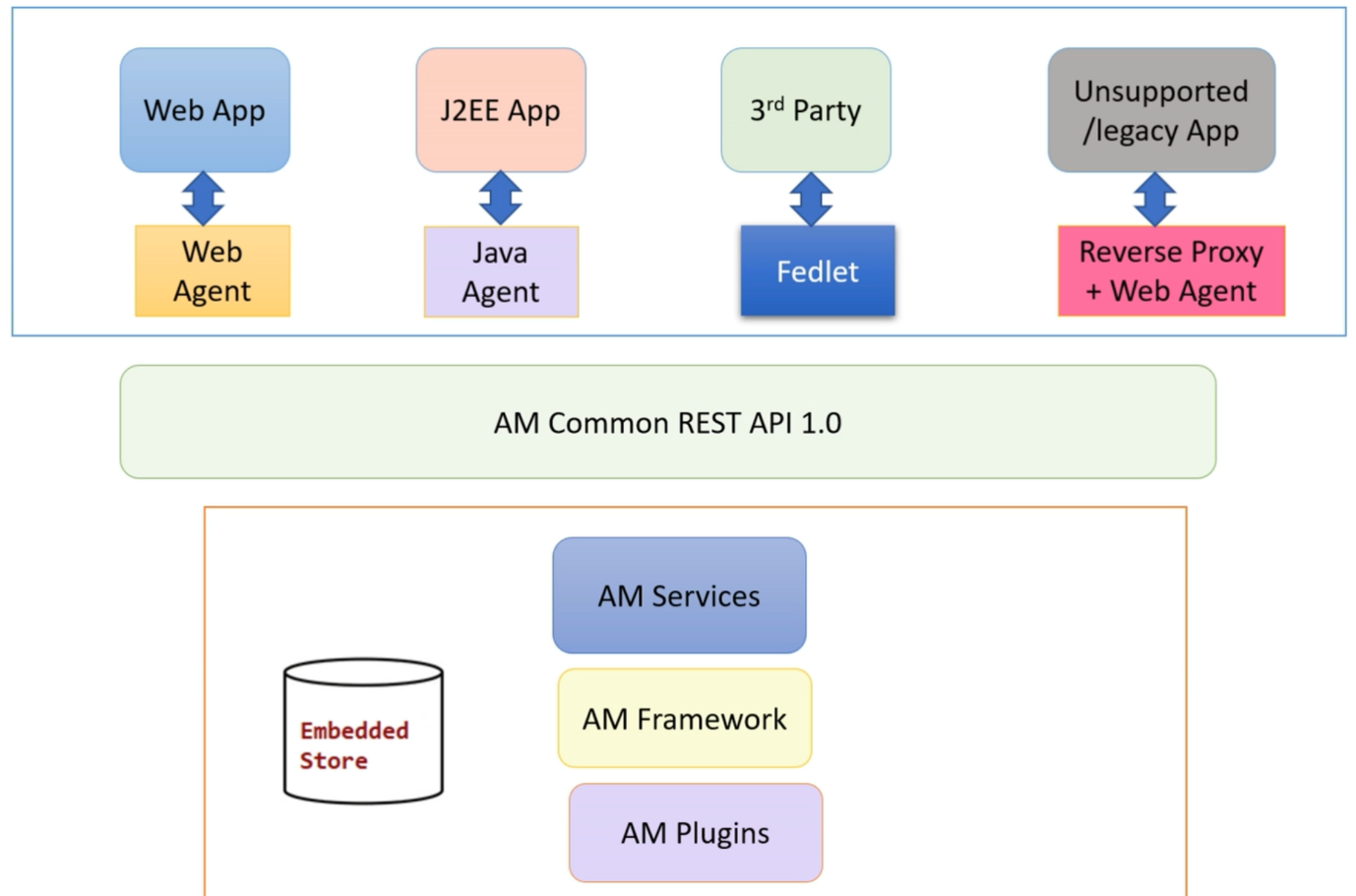
1. Authentication
2. Authorization

**Authentication Mechanism**

Authentication Mechanism is a way by which a user can authenticate to the Open AM. There are various ways of Authentication Mechanism:

1. **Form Based Authentication (Facebook login):** In this a form is provided to the user based on which the user is validated and authenticated before he can use the system.
2. **Risk Based Authentication [RBA]:** It calculates the level of risk based on given login attempts and based on the risk score. It presents authentication challenge to user. In Google it happens the same, when the device is changed, it will immediately send you a mail warning about the suspicious activity. Also, there are other checks such as doing multi-factor authentication and ask you to prove yourself. For this you need to select the risk factor such as change of IP address, new device, login country etc. The second step, would be to decide what action to take, when the risk factor is detected like Captcha, 2 factor authentication.
3. **OTP Based Authentication:** It is valid only for one login session.

**Access Manager Architecture:**



Access Manager is a centralized Access Manager server, which is mainly designed for protecting resource, providing authentication, providing authorization, web security, federation and others. From the above diagram, it is clear that

1. First layer consists of different kinds of applications and their corresponding agents. Agents helps applications to talk to AM (Access Manager) Layer.
2. For some applications, agents are not sufficient there they need to use REST APIs directly use Access Manager.