Vendomatic Project

Design

Version 0.2

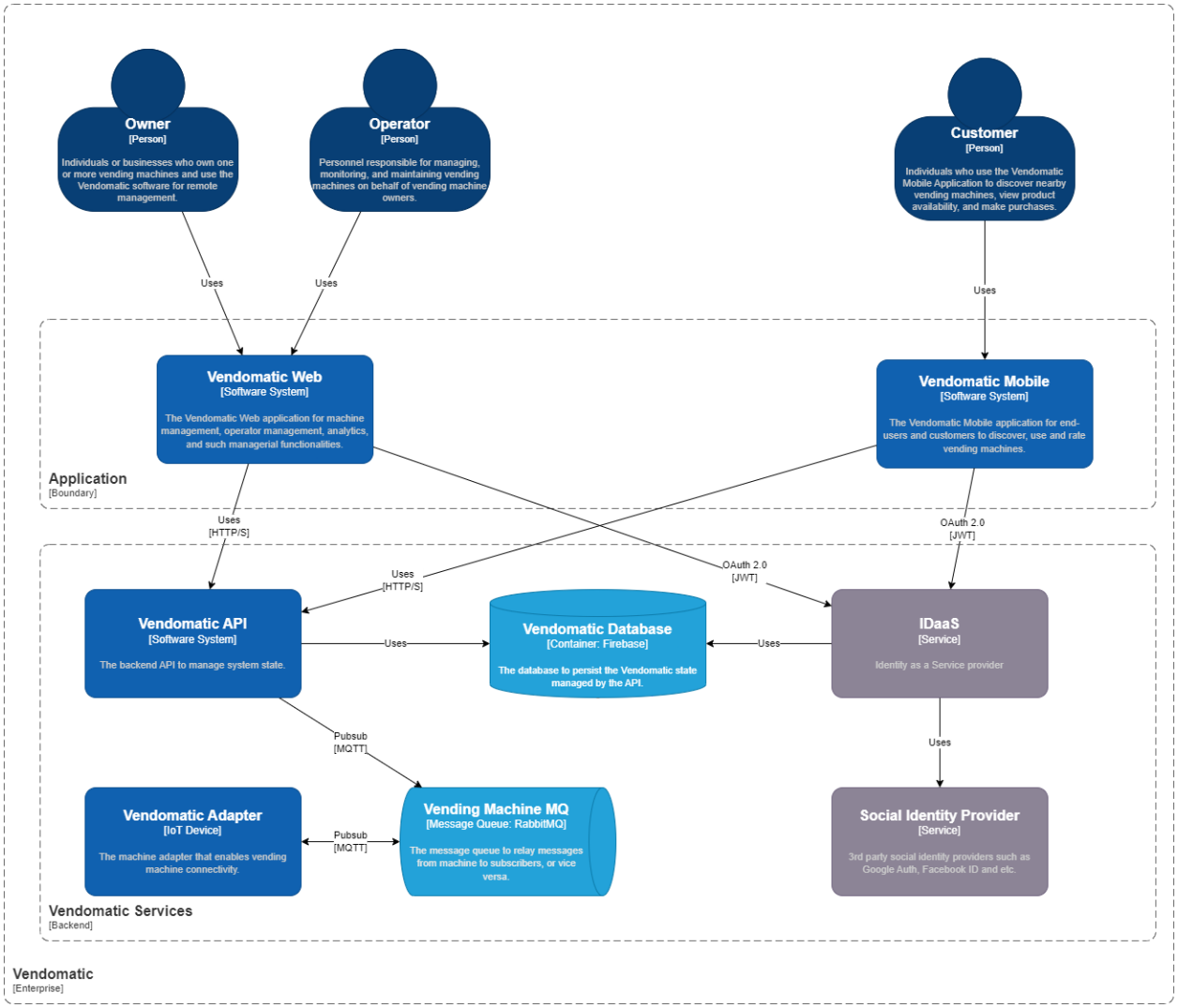
Prepared By: Code Busters

Revision History

Version	Description	Author	Date
0.1	• Draft	Kadir Kılıçoğlu	2023-04-14
0.2	• Review and format	Ezgi Özkan Tuğçe Sözer	2023-04-24

Table of Contents

1. Design Structure



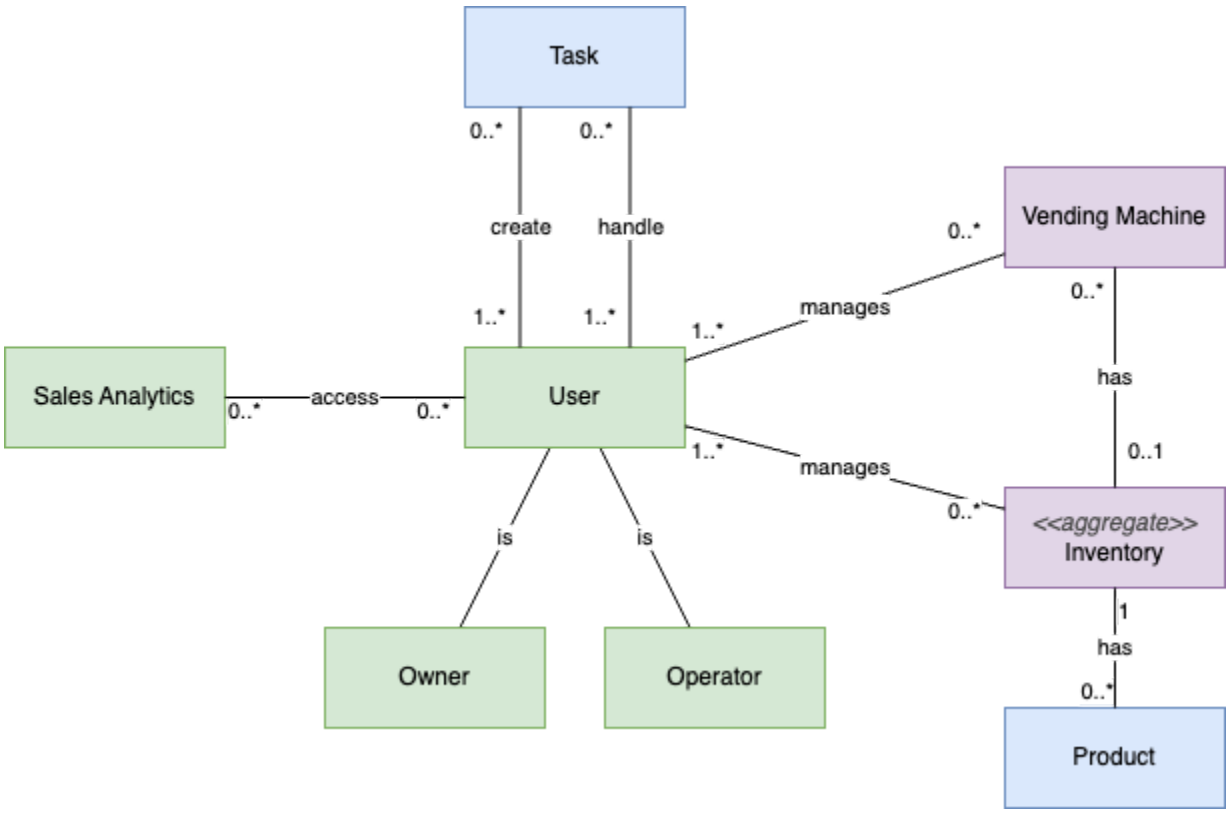
In the Vendomatic enterprise boundary there are basically 3 types of users: the owner, operator, and customer. Owners and operators interact with the web application only within the application boundary whereas the customers only interact with the mobile application.

A 3rd-party IDaaS handles the authentication and authorization, and the same service also handles social identity provider integrations.

Since the basic idea of the Vendomatic software ecosystem is based on the fact that most vending machines are disconnected, the Vendomatic Adapter proxies machine level communication across online channels through MQTT message queues.

2. Subsystems

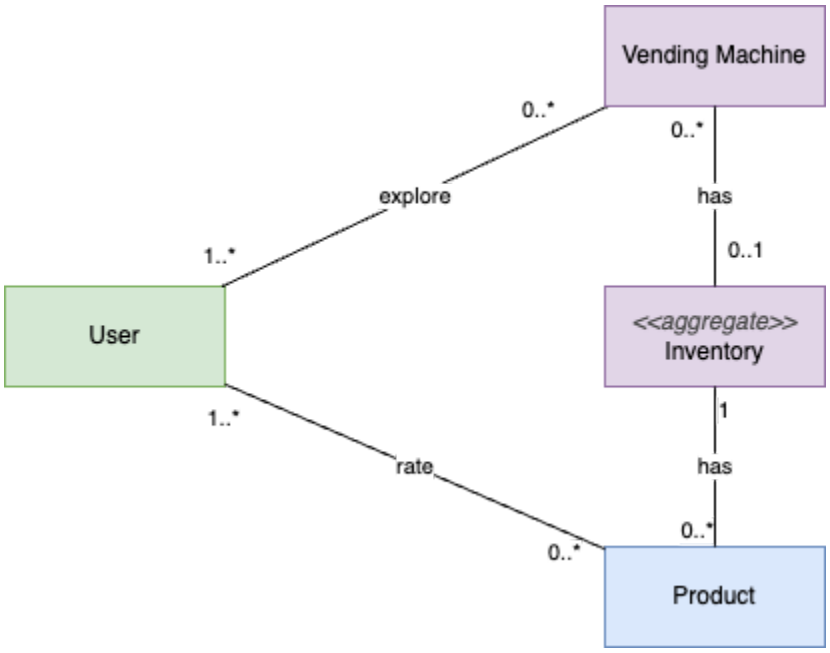
2.1. Vendomatic Web



The Vendomatic web application is a sub-system that covers the management web application for owners and operators. In this direction; a user might be an owner or an operator only. Since this is a management application, the web API supports management of tasks, machines and products over the inventory aggregate.

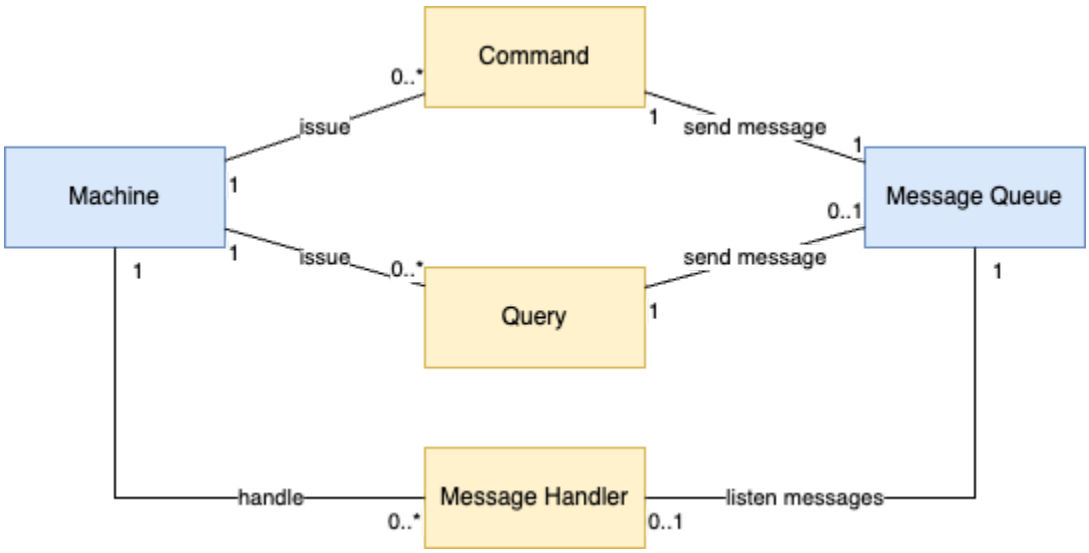
The component model depicts the major components of the Vendomatic web application which complies with the key abstractions described in the Architecture Notebook.

2.2. Vendomatic Mobile



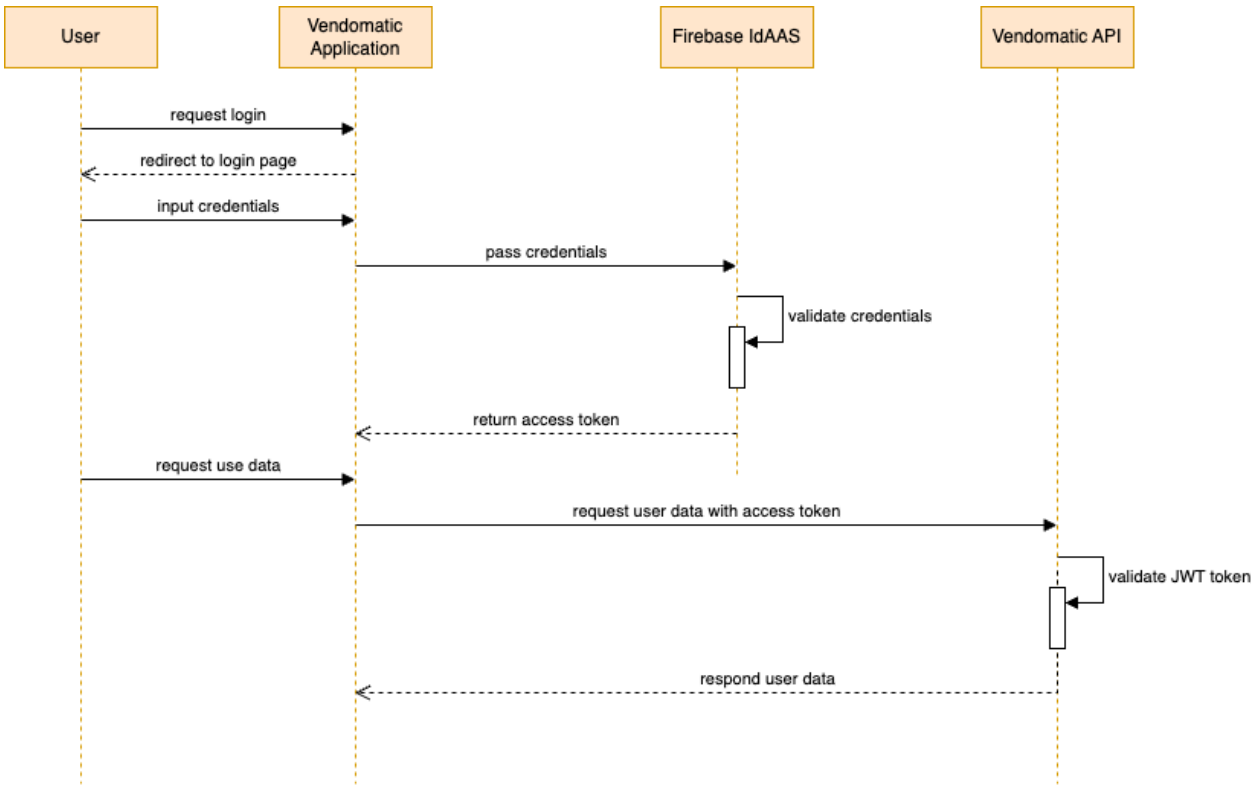
The Vendomatic mobile application targets only customers, hence the components are simplistic by its nature as seen in the component diagram above. Other than the users, the major components are the machines to be discovered and products to be rated or purchased.

2.3. Vendomatic Adapter



3. Patterns

3.1. Delegated Authentication



The Login flow is a Resource Owner Password Flow pattern common in all sub-systems. In the Resource Owner Password Flow, the client application sends a request to the authorization server that includes the resource owner's username and password. The authorization server verifies the credentials and if they are valid, issues an access token to the client application.

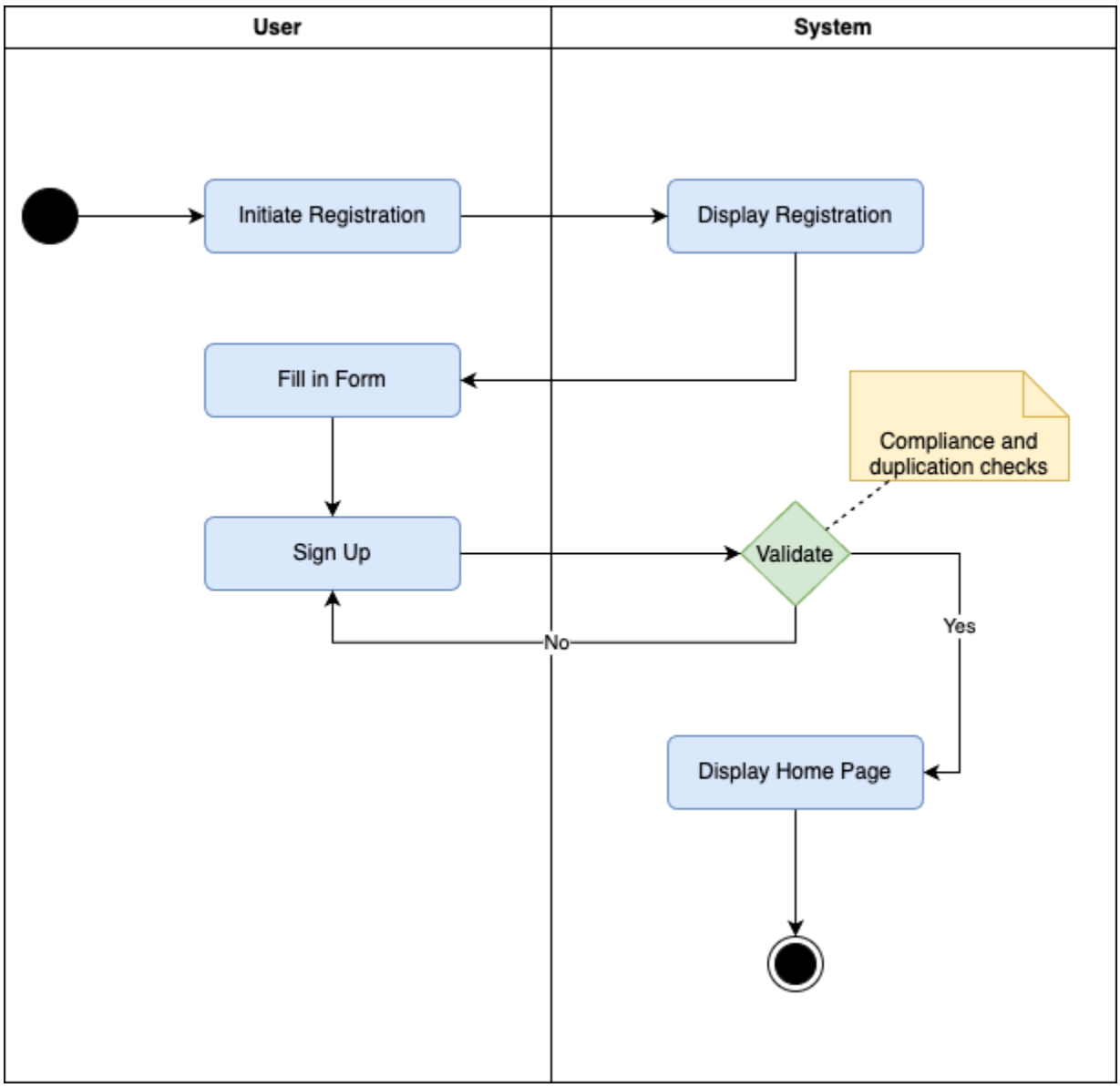
The access token is then used by the client application to access protected resources on behalf of the resource owner. The token is typically sent in the Authorization header of HTTP requests to the resource server.

One advantage of the Resource Owner Password Flow is that it allows clients to obtain access tokens without requiring a separate authentication step.

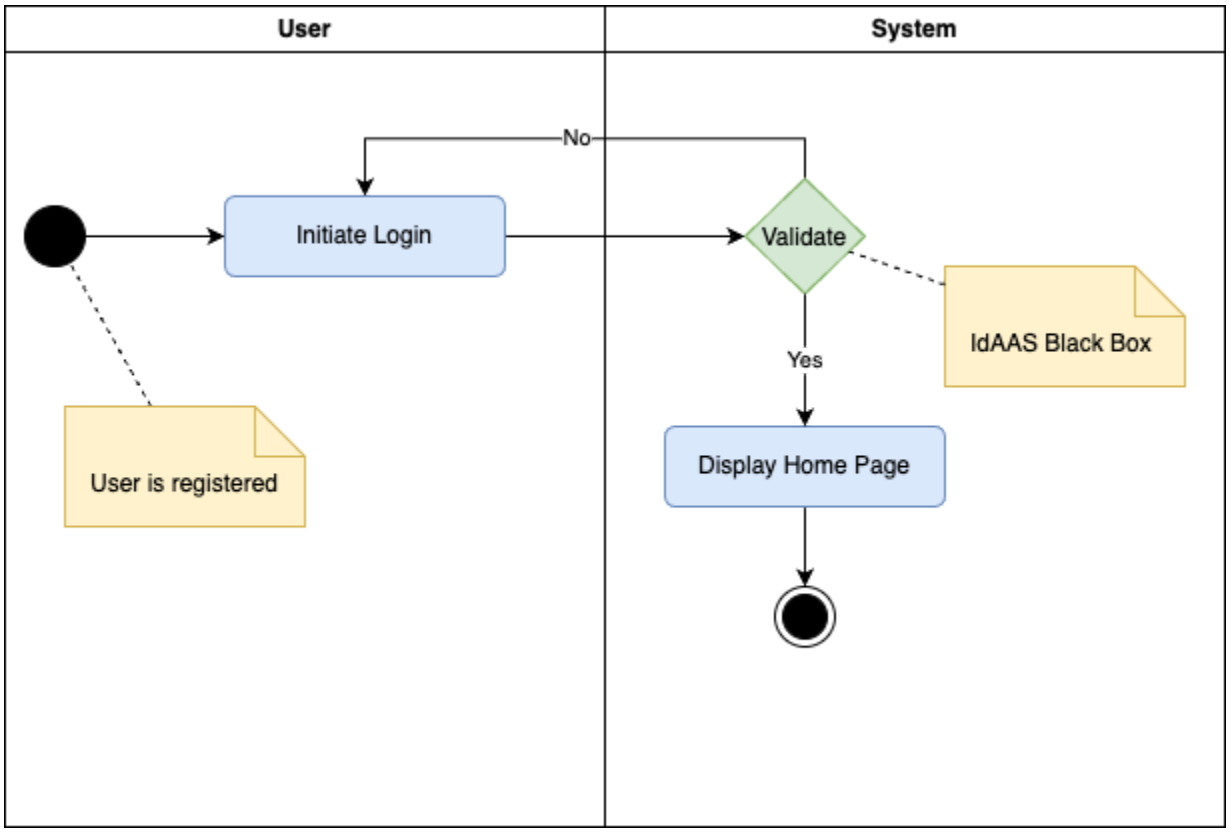
Overall, the Resource Owner Password Flow provides a simple and straightforward way for trusted client applications to obtain access tokens for accessing protected resources on behalf of the resource owner.

4. Requirement Realization

4.1. UC-08: Register to the Mobile Application



4.2. UC-08 & UC-09: Login Mobile and Web



The only difference between mobile and web logins is that the mobile login supports 3rd-party social providers. But since the authentication is handled by the IdAAS itself, and basically the process is a black box, we can depict the simple flow as the given activity diagram.