An OpenAPI Platform to Assist In-Home Care by Routing Pseudonymous Information to User-Approved Modelling Components

Joey Ambler
Supervised by
Dr Daniel Schein

Motivation

As the number of elderly people in the United Kingdom grows beyond the capacity of the National Health Service to provide in-home care for, the responsibility of caring for elderly parents often falls on their adult children.

With the growing number of Internet of Things devices in the home and other sources of data, it may be possible to develop a platform to gather information from these devices in order to make this job easier.

Aims

While developing this platform, I aim to give careful consideration to these objectives:

- Keep the solution open and general such that anyone can build a component for the platform.
- Protect the client's identity and privacy though pseudonymity and fine-grained permission management.

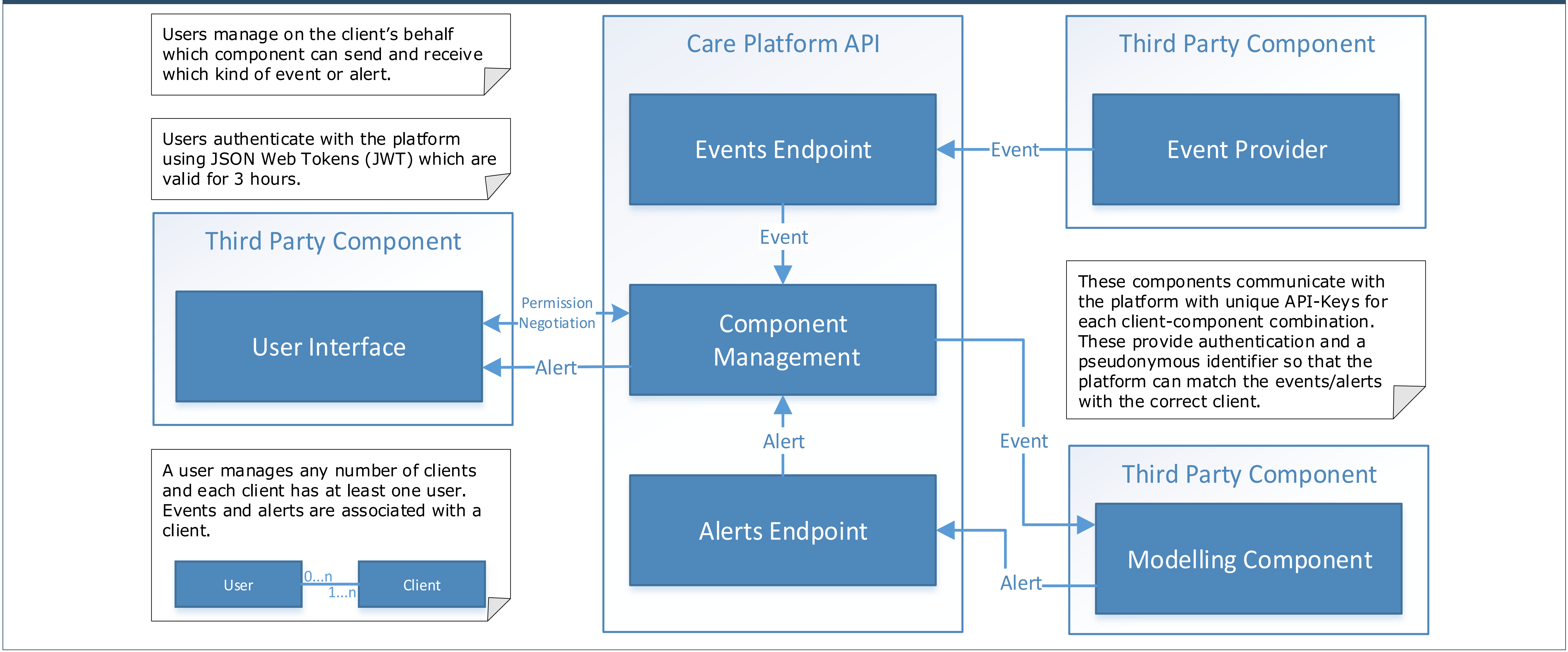
Problem Definition

I propose to build a system which is sufficiently general and open so that most relevant devices and services can interact with the platform. These devices and services (event provider components) will generate events to send to the platform. The platform will then forward these events to a modelling component, which may return an alert should the event indicate a cause for concern.

To address privacy concerns, a user (managing one or more clients) will register each event provider component and modelling component to a specific client. Each client-component pair will have:

- A unique key, which the component will use for authentication with the platform and the platform will use to match the data with the relevant client. This key mechanism will provide a pseudonymous identifier for the component to use in managing its data, without revealing the client’s identity.
- A set of permissions which detail which types of alert and event the component can send and receive.

System Overview


Users manage on the client’s behalf which component can send and receive which kind of event or alert.
Users authenticate with the platform using JSON Web Tokens (JWT) which are valid for 3 hours.
Third Party Component
User Interface
A user manages any number of clients and each client has at least one user. Events and alerts are associated with a client.
User
0...n
1...n
Client
Permission Negotiation
Alert
Care Platform API
Events Endpoint
Event
Component Management
Alert
Alerts Endpoint
Event
Third Party Component
Event Provider
These components communicate with the platform with unique API-Keys for each client-component combination. These provide authentication and a pseudonymous identifier so that the platform can match the events/alerts with the correct client.
Event
Third Party Component
Modelling Component
Alert

Work Completed So Far

OpenAPI specification and Node.js implementation for:

- User and Client Management
- Component Management with Pseudonymous Identifiers
- Permissions Management
- Events Endpoint

Future Work

- Alerts Endpoint
- Example Event Provider
- Example Modelling Component
- Further Anonymity Enforcement, K-Anonymity?
- User Interface?

Problems and Challenges

- Had to backwards port the OpenAPI specification 3.0.0 specification to Swagger/OpenAPI specification 2.0.0 due to lack of tooling. Had to work around lack of Bearer (JWT) authentication in version 2.0.0.
- Permissions management was more complex than previously thought, the controller has the most lines of code vs other controllers.
- Correctly designing the database was a challenge, many of the relationships between entities were more complex than previously anticipated. Such as the Client-Component relationship.

Built Using

API Specification	Platform Server	Database Management
OPEN API INITIATIVE	express	Sequelize Object-Relational Mapping Tool
swagger	node JS	

University of Bristol

care.ambler.me