**Title**

Transportation App: UI Framework Date: 2023-10-14 William Black, Robert Carlson, Paul Sholter

**Status**

Approved, combination of dynamic and granular permissions.

**Context**

We are tasked with developing a mobile app for a modern transportation company, which involves multiple critical features, including geolocation services, real-time location tracking, payment processing, authentication, and more. The decision regarding how we handle permissions within the app is a crucial architectural consideration that will impact user experience and security.

**Decision**

A dynamic and granular permissions system is an approach to user permissions in an app that offers fine control based on context and user preferences. It involves dynamic permissions that adapt to the user's actions, requesting access only when necessary for specific tasks, enhancing user trust. Additionally, granular permissions provide detailed categories, allowing users to grant or deny access with precision. For instance, instead of granting access to all location data, a user might grant access to location data only while actively using the app, offering more control over their data. This combined approach ensures user control over app access, promoting privacy, security, and transparency, which is crucial for apps dealing with sensitive data. This approach is motivated by the need for user trust and privacy in various aspects of the app, such as geolocation services, real-time location tracking, map interface, payment transactions, authentication, data storage, push notifications, and security measures. It ensures a user-centric and secure experience while allowing users to manage their data and preferences.

**Consequences**

Implementing a dynamic and granular permissions system ensures that users have control over their data and provides transparency in how and when their information is accessed. This approach respects user privacy and builds trust, especially in a transportation app that handles sensitive data and real-time tracking. It requires clear user communication to explain why certain permissions are necessary, making the app more user-friendly. By following best practices for security and data protection, we ensure the app complies with industry standards and keeps user data secure.