gluu

Department for Work & Pensions

UK DWP Attribute Exchange Pilot

Why Gluu was selected

DWP evaluated several identity software vendors. For the pilot, it was determined that the Gluu platform offered the most comprehensive implementation of the User Managed Access (UMA) protocol.

Specifically, the Gluu platform could implement a claims gathering endpoint easily out of the box and it could act as an UMA Resource Server (RS). So from a deployment standpoint, Gluu offered the quickest path to completing a minimum viable product by reducing the software development required by DWP.

The results

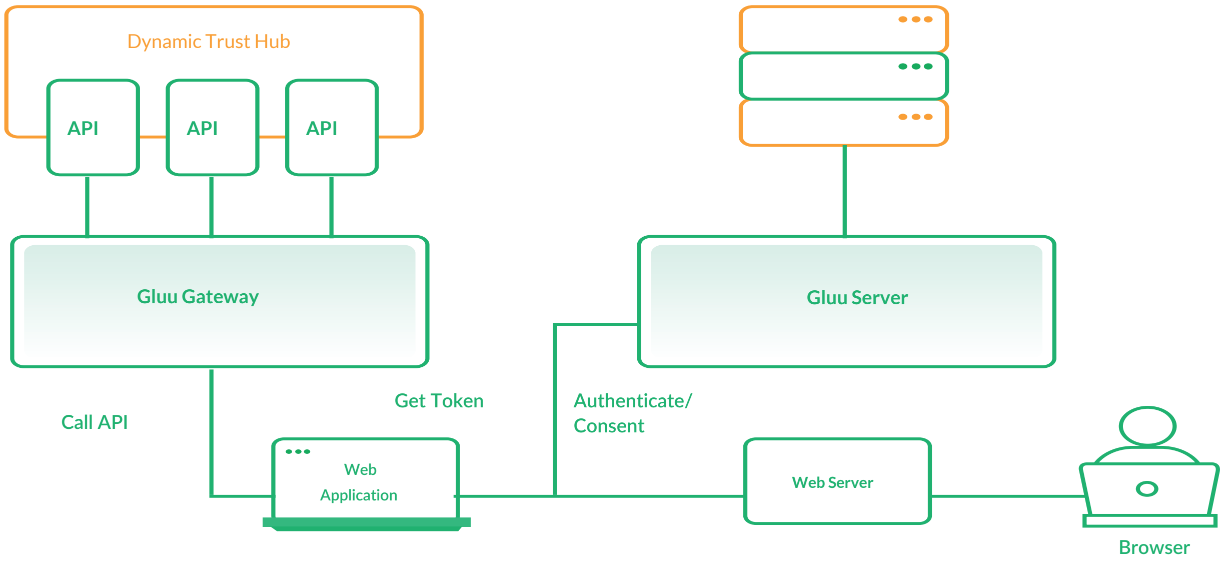
After several weeks of development, DWP was able to prove that the UMA flow would achieve the desired centralization of user control over the release of personal information, and that Gluu as a software platform was capable of supporting the needs of the department around IAM as a foundation of the DTH. The use of open standards, such as UMA, is an important consideration today for government organizations to ensure enterprise scale deployments and this principle has underpinned the development of the DWP Identity Strategy.

Objective

The Department for Work and Pensions (DWP) is responsible for welfare, pensions and child maintenance policy. As the UK's biggest public service department it administers the State Pension and a range of working age, disability and ill health benefits to around 20 million claimants and customers. One of its responsibilities is to confirm eligibility for "Blue Badges," which enable people with disabilities or health conditions to park on-street closer to their destination. The rollout of a new Blue Badge technology stack drove the need for new APIs that enabled authorized government departments to write software to automatically access information about the badge holder. It was important that the badge holder consented to share their information, enabling them to control the release of personal and health information. This project was undertaken by DWP Identity & Trust Delivery hub based in Sheffield. The team consisted of architects, developers, devops engineers, and project managers.

Business challenges that drove the project forward

The Blue Badge requirement aligned with an effort previously under development by DWP called the Dynamic Trust Hub (DTH), which consists of a number of interoperable services aimed at providing secure verification of people's identities. Protecting the DTH APIs was a challenge. Standards like OAuth 2.0 enable protection of an API using scopes. But what is the best way to protect APIs using OAuth that would enable DWP to interact directly with the user post-authentication? At the same time, one-off technology solutions are hard to maintain in the long term. So how could DWP align with existing security standards with a range of vendors who could support it?


Dynamic Trust Hub
API
API
API
Gluu Gateway
Gluu Server
Call API
Get Token
Authenticate/
Consent
Web
Application
Web Server
Browser