Handling Authentication and Authorization

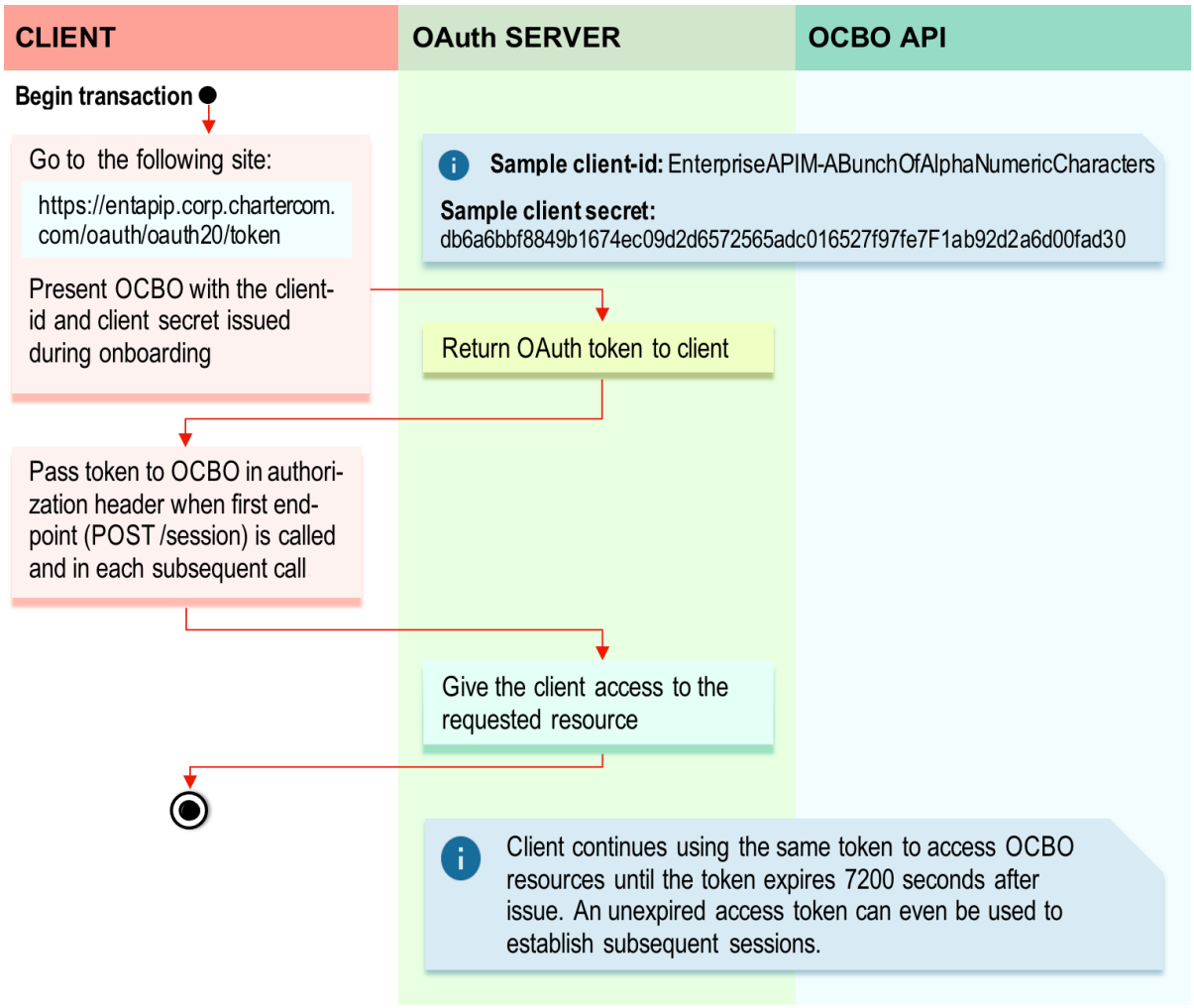
Authetication and authorization are both security measures necessary to allow a client to access resources. But there's one key difference: authentication pertains to identity, whereas authorization is tied to actions. Authentication proves that the party making the API call is a trusted retail partner, not some bot looking for security vulnerabilities. Authorization then dictates which resources the authenticated client can access.

Using OAuth 2.0 Protocol

OAuth 2.0 is an open source, industry-standard authorization protocol that gives an API client limited access to protected server resources. Spectrum is the resource owner in this case—that is, the owner of the OCBO API and its data. We use the OAuth framework to give third parties access to OCBO and its assets.

Access Tokens

The OAuth authorization server gives clients secure access to API resources by means of an access token. The process of requesting a token is shown in the image below:



Tokens let clients use the API without complicated password protocols or other clunky credentialing methods. They also protect the server from unauthorized access. Issuing a token is a bit like giving a keycard to a hotel guest. The API relies on OAuth to generate a room key, of sorts: a JSON web token, or JWT. It's a string with a limited scope and lifespan. Like a hotel keycard, it's good only for a specified period of time.