Applications with MIT's OpenID Connect Server

The MIT OpenID Connect Server (oidc.mit.edu, OIDC) can be used to provide authentication of end users using OpenID Connect and authorization of API access using OAuth 2.0.

Server Information

The MIT OIDC server supports an extended version of OpenID Connect Registration and the server's discovery document is available at https://oidc.mit.edu/.well-known/openid-configuration. This JSON document contains all key information for the server and is meant to be fetched directly by client applications.

The issuer for the MIT OIDC server is the same as its base URL, https://oidc.mit.edu/. (Note the trailing slash)

The server's public key is available in JSON Web Key format at https://oidc.mit.edu/jwk.

End users can log in to the MIT OIDC server using their MIT username and password or a valid Kerberos ticket.

Token Information

All tokens issued from the MIT OIDC server are JSON Web Tokens (JWTs) signed with JSON Web Signatures (JWS) using the server's public key.

Related Articles:

- Logging in users to your application using OpenID Connect
- Protecting APIs with OAuth 2.0