# 11. Baseline API Security

## 11.1 VA Standards

## User Identity Authentication Enterprise Design Pattern - <https://www.oit.va.gov/library/programs/ts/edp/privacy/UserIdentityAuthentication_V2.pdf>

## Secure Messaging Enterprise Design Pattern (this is dated) - <https://www.oit.va.gov/library/programs/ts/edp/privacy/SecureMessaging_V2.pdf>

## 11.2 OAuth 2.0 and OpenID Connect Security

## Identity and Access Management (IAM) has implemented OAuth 2.0 services to allow API consumers to pass an OAuth token to APIs.  API gateways and API implementers can take advantage of the OAuth validation and session profile services to ensure tokens presented are valid and obtain information about the authenticated user.  An example end to end walkthrough of an OAuth Grant Code implementation using the IAM SSOe OAuth service can be found here (<https://vaww.oed.portal.va.gov/sites/vrm/IAM/playbooks/Pages/SSOe/OAuth%20Code%20Grant.aspx>).

## More information can be found at the links below:

## Single Sign-On External - <https://vaww.oed.portal.va.gov/sites/vrm/IAM/playbooks/Pages/SSOe/SSOe.aspx>

## OAuth – <https://vaww.oed.portal.va.gov/sites/vrm/IAM/playbooks/Pages/SSOe/OAuth.aspx>

## Single Sign-On Internal – <https://vaww.oed.portal.va.gov/sites/vrm/IAM/playbooks/Pages/SSOi/SSOi.aspx>

## OAuth – service coming soon

## Note: All integration with Enterprise Services (ES), including IAM, require submission of a Service Request (SR) prior to beginning any work (<https://escp.aac.va.gov/>).

## 11.3 API Security Guidelines and Best Practices

OAuth 2.0 Threat Model and Security Considerations (<https://tools.ietf.org/html/rfc6819>).

API Security

The Projects when going through intake have to get an App code for the proper tagging of resource in use. The process for intake to create App code triggers the creation of the initial AD objects to include the Site Service and User objects for Distribution lists, Security Groups, and OUs.

The Ability to access the environments is via elevated privileges to the Cloud hosted systems to administer, Manage and access developer tool sets.

The Project must create the proper Security groups that are managed via a Service Now incident ticket, and the application team managing the application.

The procedure to have access to APIs and Development is:

1. Must have elevated privileges
2. Must have the token and NEMA
3. Must be enrolled through Clarify (Linux)
4. Use of EPAS to add users to the proper Security groups created at time of intake or with a Service Now incident
5. The users added to the security groups are reduced to the least privilege access to the Role within the API development solution
6. The Cloud Service Providers have other authentication mechanisms and security controls to ensure reduced access for only those roles privileges

The Use of centralized 2 factor access for Git Hub repositories.

1. Access account request
2. Access 3rd party approver
3. Use of a mobile 2 factor authentication app
4. Log on to the specifically shared GitHub repository