# 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>).