What is it?


- Complements and enhances RFC 6819
- Systematically captures additional security threats and respective mitigations
- Recommends mitigations beyond security considerations in RFC 6749
Recommendations

- Exact redirect URI matching at AS (token leakage)
- Avoid any redirects or forwards, which can be parameterized by URI query parameters (open redirection)
- One-time use tokens carried in the STATE parameter for CSRF prevention
- AS-specific redirect URIs (mix-up)
- Clients shall use PKCE (or nonce) to prevent code injection/replay
- TLS-based methods for sender constraint access tokens (token replay)
- Use end-to-end TLS whenever possible (token leakage)
- Access Token Privileges Restriction (privilege escalation) NEW
Implicit Grant & Access Token Replay NEW

- Options to protect implicit grant are in an early stage of adoption
  - Token binding
  - JARM
- Recommendation: use Authorization code instead of implicit
  - OpenID Connect clients may use response type "token id_token" and "nonce"
- Single Page Applications can be built with authorization code due to CORS