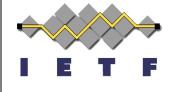
OAuth 2.0 Token Binding



Brian Campbell Michael B. Jones John Bradley William Denniss



London
March 2018

draft-ietf-oauth-token-binding

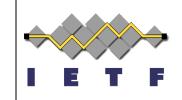
https://tools.ietf.org/html/draft-ietf-oauth-token-binding-06



Token Binding Overview

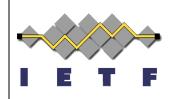
- Enables a long-lived binding of cookies or other security tokens to a client generated public-private key pair
- Use is negotiated in TLS handshake via TLS extension
- Possession of key is proven by signing the TLS exported keying material (EKM) and sending as an HTTP header in every request
- Cookies and tokens can be bound to the key
- Key is scoped to the effective top-level domain + 1
- Federated/cross-domain use-cases supported via referred token binding (vs. provided)

OAuth 2.0 Token Binding in a Nutshell



- Provide an OAuth 2.0 proof-of-possession mechanism based on Token Binding to defeat (re)play of lost or stolen tokens
 - Bind access tokens with referred Token Binding ID
 - Representation in JWT access tokens and introspection responses ("cnf" confirmation claim with a "tbh" token binding hash member)
 - Bind refresh tokens with provided Token Binding ID
 - Bind authorization codes via PKCE
 - Native app clients
 - Web server clients
 - Binding for JWT Authorization Grants and JWT Client Authentication

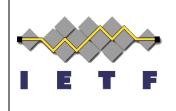
Changes since Singapore



- Draft -06
 - Use the boilerplate from RFC 8174
 - Update refs: draft-ietf-tokbind-https to -12 & draft-ietf-oauth-discovery to -09
 - Minor editorial fixes



Looking Ahead



- Token Binding documents progress to RFC
 - For real this time (maybe)
- Implementation experience and feedback
 - This stuff should be really easy once the hard parts are done