Workgroup:	Web Authorization Protocol
Internet-Draft:	draft-ietf-oauth-security-topics-17
Published:	6 April 2021
Intended Status:	Best Current Practice
Expires:	8 October 2021

Authors:	T. Lodderstedt	J. Bradley	A. Labunets	D. Fett
	yes.com	*Yubico*		*yes.com*

OAuth 2.0 Security Best Current Practice

OAuth 2.0 Security Best Current Practice

- Describe the best current security practice for OAuth 2.0
- Update and extend the OAuth 2.0 Security Threat Model
- Incorporate experience from practice and research
- Cover new threats relevant to OAuth 2.0, in particular in high-risk environments like banking, eID

Status:

- First WGLC end of last year on version -13
- Last interim meeting on -16
- Current version: -17

What’s new since -16?

New: Use of Metadata RECOMMENDED

- For both servers and clients
  - Reduces configuration mistakes impacting security,
  - facilitates better mix-up protection,
  - improves developer experience.
- Using metadata is the RECOMMENDED way to announce PKCE support
  - Important to let client know that it can rely on PKCE.
  - Before: either metadata or deployment-specific way.

New: Minor Security Improvements

- AS MUST NOT expose open redirectors.
  - Before: Limited to clients.
- AS MUST reject non-https redirect URIs
  - Exception: Native client URLs pointing to same device (w/ localhost URI or custom scheme)
- Security model clarification: Attackers can collaborate with each other.

New: Improved Mix-Up Mitigation

Previous Recommendation: Use separate redirect URIs per issuer!

- \+ based on existing OAuth features
- \- not suitable for schemes with centralized client registration (open banking!)
- \- needs a lot of explanation for developers
- \- easy to get wrong
- \- hard to automate in libraries

New: Improved Mix-Up Mitigation

Draft: draft-ietf-oauth-iss-auth-resp-00

Defines the `iss` parameter in the authorization response (+ metadata flag).

- \+ Simple mechanism
- \+ Formally proven security against mix-up attacks
- \+ Easy to automate in libraries when metadata flag is evaluated

New: Improved Mix-Up Mitigation

Mitigation is REQUIRED when Client interacts with multiple AS

RECOMMENDED

Mix-up defense via Issuer Identification

Default

draft-ietf-oauth-iss-auth-resp

With OIDC or JARM

Use existing `iss` Claim

Processing details in draft-ietf-oauth-iss-auth-resp

Alternative

Per-Issuer Redirect URIs

Processing details in
draft-ietf-oauth-security-topics

Status of the Document

- All important areas now covered - robust solution for mix-up
- Actionable recommendations
  - Foundation for security of OAuth 2.1
  - OpenID FAPI 2.0 aligned with Security BCP
- Future topics (out of scope for now):
  - Specifics of mobile environments → update BCP 212 (RFC 8252)?
  - Higher security level, new security model → new topics for future updates of the BCP

Ready for next WGLC!

Q&A