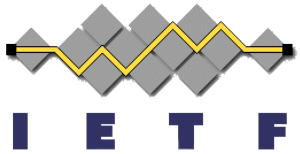
A Token Binding method for OAuth 2.0 Proof Key for Code Exchange

Brian Campbell
John Bradley
Michael Jones

IETF 96
Berlin
July 2016

current: https://tools.ietf.org/html/draft-campbell-oauth-tbpkce-00

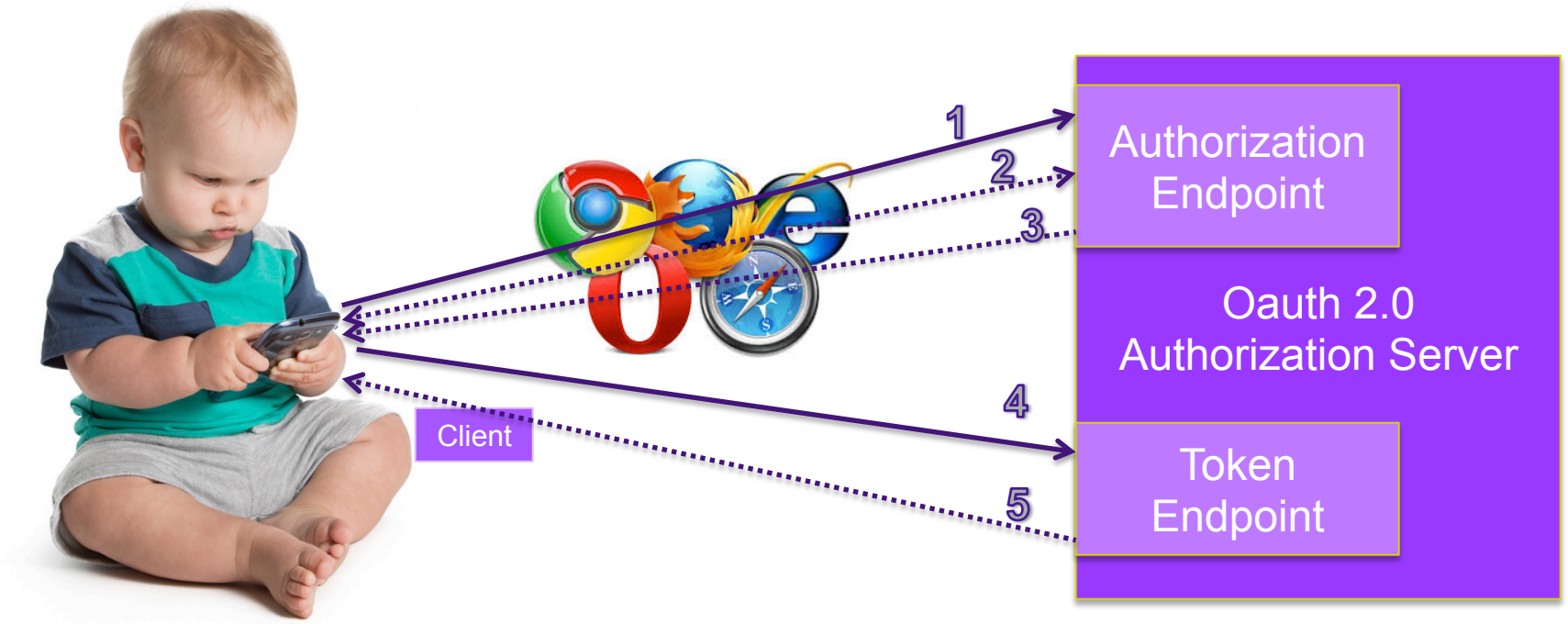
Token Binding Review



- Uses a public-private key pair generated by the client to sign TLS exported keying material and create long-lived TLS binding
- draft-ietf-tokbind
  - -negotiation-03
    - TLS extension for token binding protocol negotiation
  - -protocol-08
    - Token Binding protocol message format
  - -https-05
    - Embedding token binding messages in HTTPS

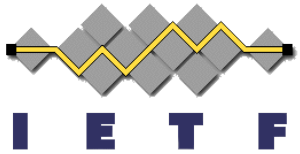
PKCE Review

- RFC 7636: **P**roof **K**ey for **C**ode **E**xchange by OAuth Public Clients (pronounced "pixy")
- Mitigation of authorization code interception attack for native OAuth clients



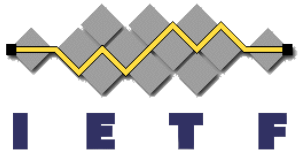
1. Authorization request + **code_challenge** & **code_challenge_method**
2. Authenticate and approve
3. Authorization response w/ code
4. Token request w/ code + **code_verifier**
5. Token response w/ access & refresh token

What is TBPKCE?



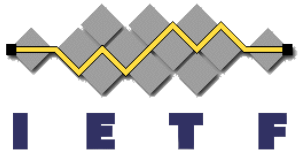
- Using token binding to do a variation of PKCE
- Authorization Request (Code Challenge)
  - “code_challenge” is the base64url encoding of the SHA-256 hash of the Provided Token Binding ID that the client will use when calling the authorization server's token endpoint
  - “code_challenge_method” is “tb2”
- Access Token Request (Code Verifier)
  - "Sec-Token-Binding" header with Token Binding Message and Provided Token Binding ID
  - “code_verifier” is “provided”

Why Bother?



- That's a good question…
- Is this token bound code materially better than PKCE's S256?
- We've started looking at Token Binding + OAuth across the board (also OpenID Connect)
  - Not as much value as binding access, refresh, and ID tokens but still a piece of the overall

Next Steps?



- That's also a good question…
  - Kill it?
  - Move forward with it?
    - As an OAuth WG document?
    - As part of the other TB document?
  - Let it marinate for a while before deciding?
  - Other?
- Read it!
  - It is very very short (https://tools.ietf.org/html/draft-campbell-oauth-tbpkce-00)
  - Feedback, changes, additions, vague & incomprehensible criticisms are always welcome (kinda)