OAuth 2.0 Token Binding

Brian Campbell
Michael B. Jones
John Bradley

IETF 100
Singapore
November 2017

draft-ietf-oauth-token-binding

https://tools.ietf.org/html/draft-ietf-oauth-token-binding-05

The Setting of the Context

Provide an OAuth 2.0 proof-of-possession mechanism based on Token Binding to defeat (re)play of lost or stolen tokens (access, refresh, authorization codes, etc.)

from IETF 96

Quick Refresher on -04

- Token Bind access tokens with referred Token Binding ID
  - Representation in JWT access tokens and introspection responses
- Token Bind refresh tokens with provided Token Binding ID
- Token Bind authorization codes via PKCE
  - Native app clients
  - Web server clients

Dependency Status

- Token Binding WG documents; -tokbind-negotiation, -tokbind-protocol, and -tokbind-https are all very close to RFC publication
  - I may have said something similar in Prague…
  - But all have been Submitted to IESG for Publication and are in AD evaluation

Brian Campbell
@__b_c

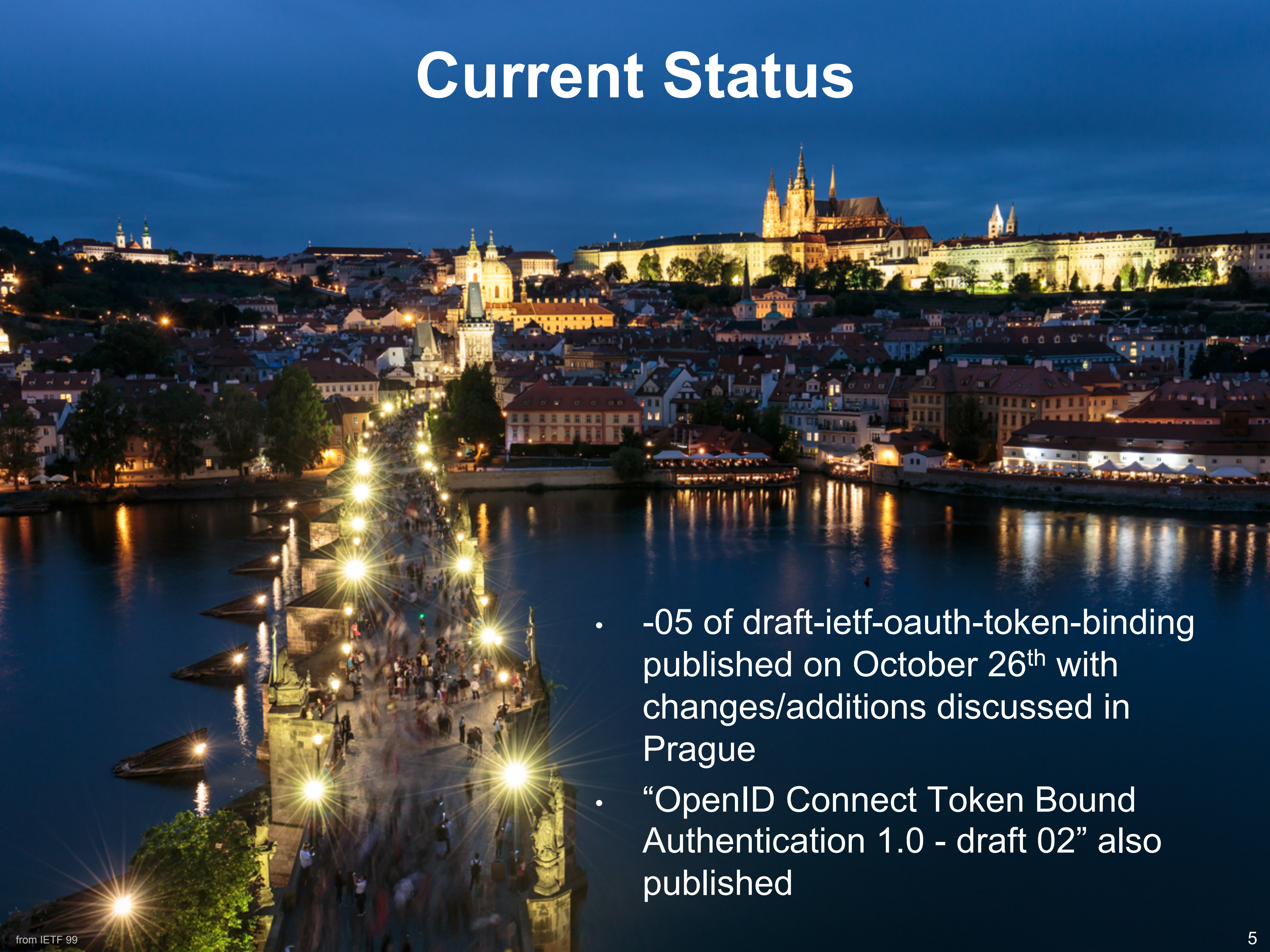
#ietf92 with @ve7jtb & @leifjohansson chairing the initial Token Binding WG meeting

RETWEETS 5 LIKES 2

8:16 AM - 24 Mar 2015

from IETF 92

Current Status



from IETF 99

- -05 of draft-ietf-oauth-token-binding published on October 26th with changes/additions discussed in Prague
- "OpenID Connect Token Bound Authentication 1.0 - draft 02" also published

Changes in -05

- Specify that authorization servers don’t token bind refresh tokens issued to a client that doesn't support bound refresh tokens
  - Support indicated by the client metadata parameter or via ‘static’ registration information
  - Added security considerations on unbound refresh tokens
    - Potentially infeasible for some distributed web-based confidential clients
    - RTs are indirectly bound to the client's credentials and cannot be used without the associated client authentication
- Adjust the language around aborting authorizations in the ‘Phasing in Token Binding’ text to be somewhat more general and not only about downgrades
- Remove reference to (and usage of) 'OAuth 2.0 Protected Resource Metadata', which is no longer a going concern

Changes in -05 cont.

- Added/described Token Binding for JWT Authorization Grants and JWT Client Authentication
  - JWT must have a “cnf” (confirmation) claim with a “tbh” (token binding hash) member identifying the Token Binding ID of the Provided Token Binding used by the client on the TLS connection to the authorization server
  - client_assertion_type:

    urn:ietf:params:oauth:client-assertion-type:jwt-token-bound
  - Authentication method values:
    - private_key_token_bound_jwt
    - client_secret_token_bound_jwt
  - grant_type: urn:ietf:params:oauth:grant-type:jwt-token-bound

Looking Ahead

- Token Binding documents progress to RFC
  - For real this time
- Implementation experience and feedback
- Get the band back together again for IETF 101 in London

from IETF 89