Composite Presentation:
OAuth
MTLS, Token Binding & Token Exchange

IETF 102

~~San Francisco~~

Montreal

July 2018

Brian Campbell

OAuth 2.0 Token Binding

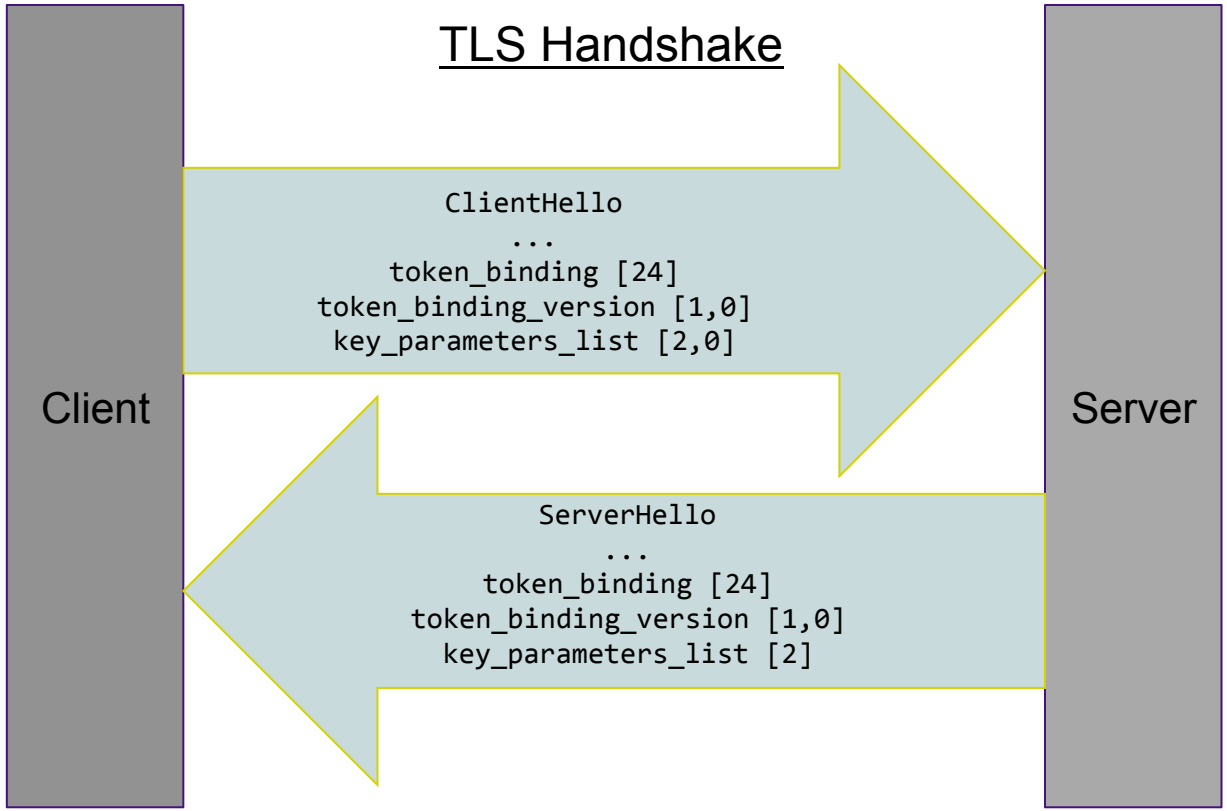
draft-ietf-oauth-token-binding-07

IETF 96, Berlin

Token Binding Overview

- Three core drafts from TOKBIND WG (last meeting this week on Friday)
  - Negotiation, Protocol, & HTTPS
- 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 an HTTP header in every request
- Cookies and other 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)

Token Binding Negotiation



Key Parameters:

(0) rsa2048_pkcs1.5
(1) rsa2048_pss
(2) ecdsap256

Also need extenstions:

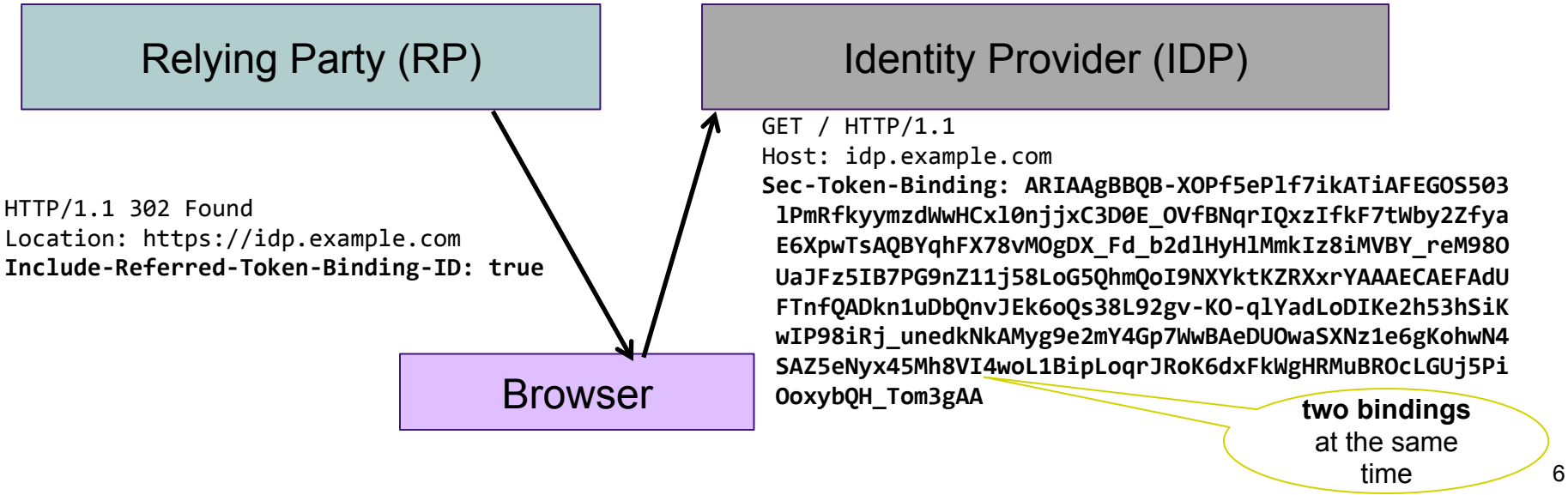
Extended Master Secret
Renegotiation Indication

Token Binding Protocol & HTTPS

- Encoded Token Binding Message
  - (1 or more) Token Bindings
    - Type (provided / referred)
    - Token Binding ID (key type and public key)
    - Signature over type, key type, and EKM (TLS **E**xported **K**eying **M**aterial)
    - Extensions
- Proves possession of the private key on the TLS connection
- Keys are long-lived and span TLS connections

Federated/Cross-Domain Token Binding

- There's an HTTP response header that tells the browser that it should reveal the Token Binding ID (the key) used between itself and the RP (referred) in addition to the one used between itself and the IDP (provided)
- And generic Token Binding implementations should be able to send referred based on other signals or preemptively too



OAuth 2.0 Token Binding Overview

- 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

Happenings since London

IETF 101, London

- Oauth Token Binding draft -07
  - Base64url encoding of the “tbh” confirmation value doesn't include any trailing pad characters, line breaks, whitespace, etc.
  - Update/fix references (internal & external)
- OpenID Connect Token Bound Authentication draft -03
  - “tbh” defined here
- Token Binding over HTTP
  - IESG state: RFC Ed Queue
- TLS Extension for Token Binding Negotiation & Token Binding Protocol
  - IESG state: Approved-announcement to be sent::AD Followup

OAuth 2.0 Mutual TLS Client Authentication and Certificate Bound Access Tokens

draft-ietf-oauth-mtls-09

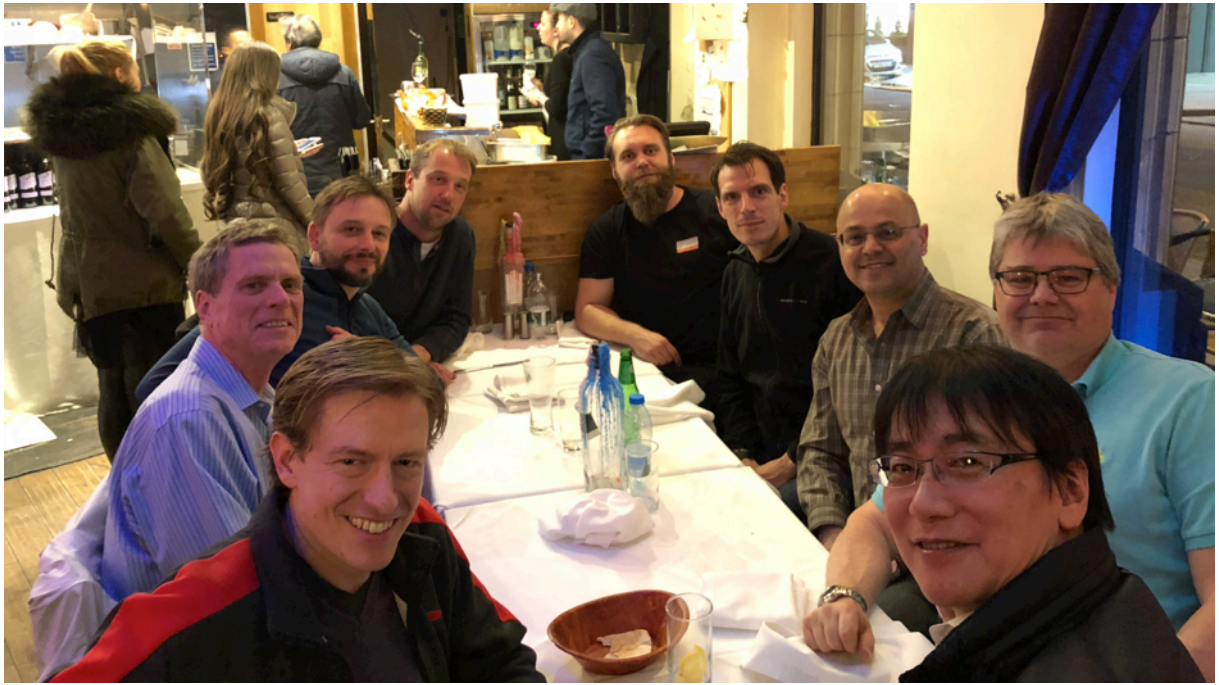
OAuth MTLS Context & Overview

- Why?
  - Enhanced security profile of OAuth 2.0 based on TLS client certificates
    - Draft is already being used by OpenBanking/PSD2esque regulatory regimes and other SDOs
- What?
  - Asymmetric key based client authentication to the AS using mutual TLS
    - Two methods: PKI based mode & Self-signed certificate based mode
  - Mutual TLS certificate bound access tokens for proof-of-possession protected resources access
    - “x5t#S256”: X.509 Certificate SHA-256 Thumbprint Confirmation Method for JWT and Introspection

Happenings since London

- WGLC done!
- Drafts -07, -08, & -09
- Numerous clarifications and editorial improvements from WGLC feedback
- Drop the use of the "sender constrained" terminology per WGLC feedback WRT to draft-ietf-oauth-pop-architecture
  - includes changing the metadata parameter name from `mutual_tls_sender_constrained_access_tokens` to `tls_client_certificate_bound_access_tokens`

Tryin' Real Hard To ~~Be~~ Find The Shepherd



IETF 101, London

OAuth 2.0 Mutual TLS Client Authent

draft-ietf-oauth-mtls-09

Status | IESG evaluation record | IESG writeups | Email expans

Versions 00 01 02 03 04 05 06 07 08 09

draft-campbell-oauth-tls-client-auth 00

draft-campbell-oauth-mtls 0(0

draft-ietf-oauth-mtls

Oct 2016 Mar 2017 Apr 2017

Document	**Type**	Active Internet-Draft (oauth WG)
	Last updated	2018-06-04
	Replaces	draft-campbell-oauth-mtls
	Stream	IETF
	Intended RFC status	(None)
	Formats	plain text xml pdf html
Stream	**WG state**	WG Document
	Document shepherd	No shepherd assigned
IESG	**IESG state**	I-D Exists

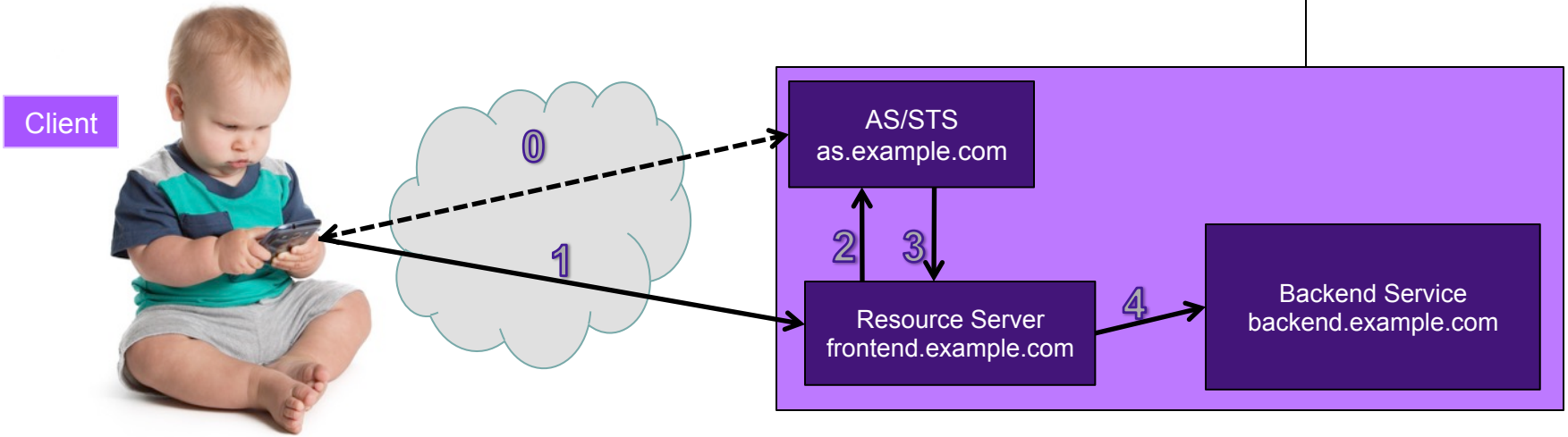
OAuth 2.0 Token Exchange

draft-ietf-oauth-token-exchange-14

An STS framework via the Token Endpoint

Attempt to Provide Context

(one example of the many many use-cases of a token exchange framework)




```
GET /resource HTTP/1.1
Host: frontend.example.com
Authorization: Bearer accVkjcJyb4BWCxGsndESCJQbdFMogUC5PbRDqceLTC
```

1

```
HTTP/1.1 200 OK
Content-Type: application/json
Cache-Control: no-cache, no-store

{
 "access_token":"eyJhbGciOiJFUzI1NiIsImtpZCI6IjllciJ9.eyJhdWQiOiJo
   dHRwczovL2JhY2tlbmQuZXhhbXBsZS5jb20iLCJpc3MiOiJodHRwczovL2FzLmV
   4YW1wbGUuY29tIiwiZXhwIjoxNDQxOTE3NTkzLCJpYXQiOjE0NDE5MTc1MzMsIn
   N1YiI6ImJjQGV4YW1wbGUuY29tIiwic2NwIjpbImFwaSJdfQ.MXgnpvPMo0nhce
   PwnQbunD2gw_pDyCFA-Saobl6gyLAdyPbaALFuAOyFc4XTWaPEnHV_LGmXklSTp
   z0yC7hlSQ",
 "issued_token_type":
     "urn:ietf:params:oauth:token-type:access_token",
 "token_type":"Bearer",
 "expires_in":60
}
```

3

```
POST /as/token.oauth2 HTTP/1.1
Host: as.example.com
Authorization: Basic cnMwODpsb25nLXNlY3VyZS1yYW5kb20tc2VjcmV0
Content-Type: application/x-www-form-urlencoded

grant_type=urn%3Aietf%3Aparams%3Aoauth%3Agrant-type%3Atoken-exchange
&resource=https%3A%2F%2Fbackend.example.com%2Fapi%20
&subject_token=accVkjcJyb4BWCxGsndESCJQbdFMogUC5PbRDqceLTC
&subject_token_type=
 urn%3Aietf%3Aparams%3Aoauth%3Atoken-type%3Aaccess_token
```

2

```
GET /api HTTP/1.1
Host: backend.example.com
Authorization: Bearer eyJhbGciOiJFUzI1NiIsImtpZCI6IjllciJ9.eyJhdWQ
   iOiJodHRwczovL2JhY2tlbmQuZXhhbXBsZS5jb20iLCJpc3MiOiJodHRwczovL2
   FzLmV4YW1wbGUuY29tIiwiZXhwIjoxNDQxOTE3NTkzLCJpYXQiOjE0NDE5MTc1M
   zMsInN1YiI6ImJjQGV4YW1wbGUuY29tIiwic2NwIjpbImFwaSJdfQ.MXgnpvPMo
   0nhcePwnQbunD2gw_pDyCFA-Saobl6gyLAdyPbaALFuAOyFc4XTWaPEnHV_LGmX
   klSTpz0yC7hlSQ
```

4

Happenings since IETF 99

- Drafts -10, -11, -12, -13, -14
- The "act" claim: only the top-level claims and the current actor are to be considered in applying access control decisions
- Several clarifications and editorial improvements suggested during AD review
- “scope” and “client_id” claim names updated to be consistent with RFC 7662 Token Introspection (was “scp” and “cid”)
- token type URIs for base64url-encoded SAML 1.1 and SAML 2.0 assertions
- No native support for validating or issuing access tokens from other authorization servers (same as it’s always been)
- IESG state: AD Evaluation::Point Raised - writeup needed

Don’t want to talk about this in Bangkok…

IESG state AD Evaluation::Point Raised - writeup needed

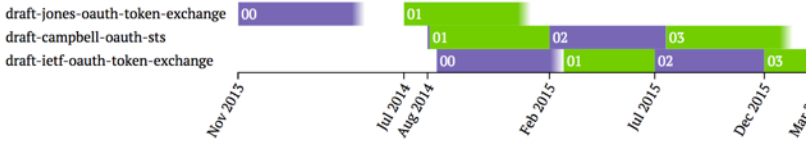
One ~~night~~ day in Bangkok circa 1999

OAuth 2.0 Token Exchange

draft-ietf-oauth-token-exchange-14

Status | IESG evaluation record | IESG writeups | Email expansions | History

Versions: 00 01 02 03 04 05 06 07 08 09 10 11 12 13 14



Document	**Type**	Active Internet-Draft (oauth WG)
	Last updated	2018-06-04
	Replaces	draft-jones-oauth-token-exchange, draft-campbell-oauth-sts
	Stream	IETF
	Intended RFC status	Proposed Standard
	Formats	plain text | xml | pdf | html | bibtex
Stream	**WG state**	Submitted to IESG for Publication (*wg milestone: May 2017 - Submit 'OAuth*
	Document shepherd	Rifaat Shekh-Yusef
	Shepherd write-up	Show (last changed 2017-12-14)
IESG	**IESG state**	AD Evaluation::Point Raised - writeup needed
	Consensus Boilerplate	Unknown
	Telechat date	
	Responsible AD	Eric Rescorla


FIN
("end" in American)