Composite Presentation: OAuth
MTLS, Token Binding & Token Exchange

IETF 102
San Francisco
Montreal
July 2018

Brian Campbell

Not Montreal
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

Client

Server

TLS Handshake

ClientHello
... 
token_binding [24]
token_binding_version [1,0]
key_parameters_list [2,0]

ServerHello
... 
token_binding [24]
token_binding_version [1,0]
key_parameters_list [2]

Key Parameters:
(0) rsa2048_pkcs1.5
(1) rsa2048_pss
(2) ecdsap256

Also need extensions:
Extended Master Secret
Renegotiation Indication
Token Binding Protocol & HTTPS

**HTTP Request**

```
GET /stuff HTTP/1.1
Host: example.com
Sec-Token-Binding: AIkAAgBBQLgtRpWFPN66kxhxGrtaKrzcMtHw7HV8yMk-_MdRXJXbDMYxZCwnCASRRrmmHHHL5wmpP3bhYtOChRDbsMapfh_QAQN1He3Ftj4Wa_S_fzVns4saLfj6aBoMSQW6rLs19IIvHze7LrGjKyCfPTKXjajebsp-TLPFZCc0JTqTY5_0MBAAAA
```

- **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 Exported Keying Material)
    - 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.

Browser

Relying Party (RP)

Identity Provider (IDP)

HTTP/1.1 302 Found
Location: https://idp.example.com
Include-Referred-Token-Binding-ID: true

GET / HTTP/1.1
Host: idp.example.com
Sec-Token-Binding: ARIAAgBBQB-XOPf5ePlf7ikATiAFEGOS5031PmRfkymzdWwHCx10njxX3D0E_OVfBNqrIQxzIFkF7twby2ZfyaE6XpwTsAQBYqhFX78vM0gDX_fd_b2d1HyH1MmkIz8iMVBY_reM980UaJFz5IB7PG9nZ11j58LoG5QhmqO9NXYktKZRXXrYAAAECAEFAduFTnfQAkn1uDqnvJEk6oQs38L92gv-KO-q1YadLoDIKe2h53h5iKWIP9iRj_unedkIkAYmg9e2mY4Gp7WwBAeUDUoaSXNz1e6gKohwN4SAZ5eNyx45Mh8VI4woL1BipLoqrJRokK6dxFkWHRMBr0cLGUj5PiOoxybQH_Tom3gAA

two bindings at the same time
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

- **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
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)

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

"access_token": "eyJhbGciOiJIUzI1NiIsIntpCjI1LjIiLjIy

Client

AS/STS
as.example.com

Backend Service
backend.example.com

Resource Server
frontend.example.com

GET /resource HTTP/1.1
Host: frontend.example.com
Authorization: Bearer aocVkJcJyb4B4WcxGsdESCJQbdFMogUC5PbRDqceLTC

POST /as/token.oauth2 HTTP/1.1
Host: as.example.com
Authorization: Basic cmhWOGpsb25nLMK11Y3Vy2SlyYW5kb20to2VjcmV0
Content-Type: application/x-www-form-urlencoded
grant_type=urn:ietf:params%3Aoauth%3Agrant-type%3Atoken-exchange
&resource=https%3A%2F%2Fbackend.example.com%2Fapi%2FGET
&subject_token=ac9VkJcJyb4BMCGsdESCJQbdFMogUC5PbRDqceLTC
&subject_token_type=urn:ietf:params%3Aoauth%3Agrant-type%3Aaccess_token

GET /api/ HTTP/1.1
Host: backend.example.com
Authorization: Bearer eyJhbGciOiJIUzI1NiIsIntpCjI1LjIiLjIy

14
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

OAuth 2.0 Token Exchange
draft-ietf-oauth-token-exchange-14

One night day in Bangkok circa 1999
IETF 83, Paris (which I did not attend but was in the area)