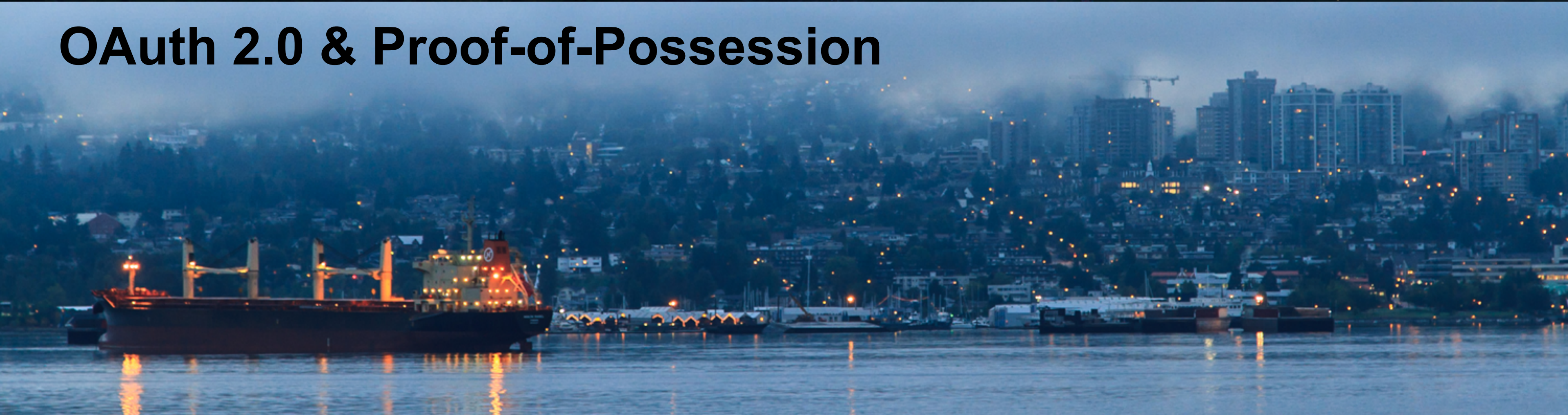
IETF OAuth WG
Virtual Interim Meeting

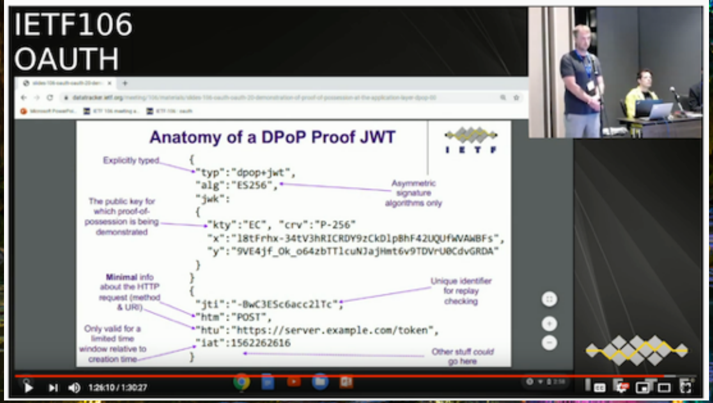
March 2020
(between Singapore
& Vancouver)



OAuth 2.0 & Proof-of-Possession

When last we met

(in person at #106 in Singapore)



Anatomy of a DPoP Proof JWT

```
{
 "typ":"dpop+jwt",
 "alg":"ES256",
 "jwk":
  {
   "kty":"EC", "crv":"P-256"
   "x":"l8tFrhx-34tV3hRICRDY9zCkDlpBhF42UQUfWVAWBFs",
   "y":"9VE4jf_Ok_o64zbTTlcuNJajHmt6v9TDVrU0CdvGRDA"
  }
}
{
 "jti":"-BwC3ESc6acc2lTc",
 "htm":"POST",
 "htu":"https://server.example.com/token",
 "iat":1562262616
}
```

Explicitly typed

Asymmetric signature algorithms only

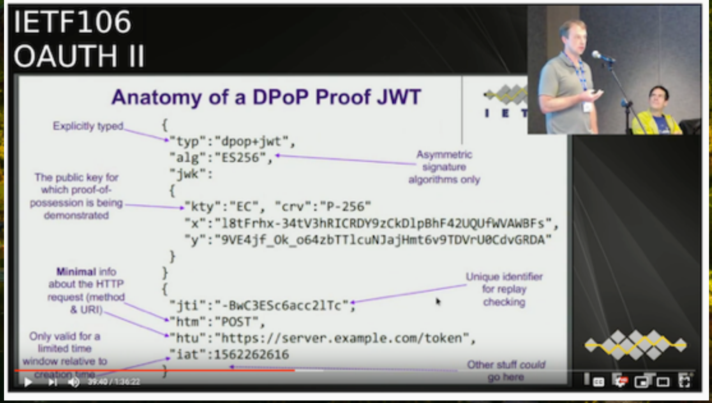
The public key for which proof-of-possession is being demonstrated

Minimal info about the HTTP request (method & URI)

Unique identifier for replay checking

Only valid for a limited time window relative to creation time

Other stuff *could* go here



Anatomy of a DPoP Proof JWT

```
{
 "typ":"dpop+jwt",
 "alg":"ES256",
 "jwk":
  {
   "kty":"EC", "crv":"P-256"
   "x":"l8tFrhx-34tV3hRICRDY9zCkDlpBhF42UQUfWVAWBFs",
   "y":"9VE4jf_Ok_o64zbTTlcuNJajHmt6v9TDVrU0CdvGRDA"
  }
}
{
 "jti":"-BwC3ESc6acc2lTc",
 "htm":"POST",
 "htu":"https://server.example.com/token",
 "iat":1562262616
}
```

Explicitly typed

Asymmetric signature algorithms only

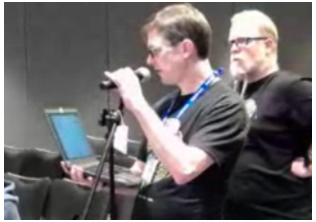
The public key for which proof-of-possession is being demonstrated

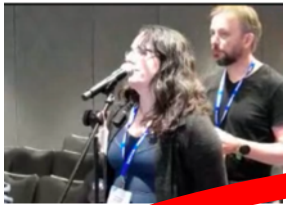
Minimal info about the HTTP request (method & URI)

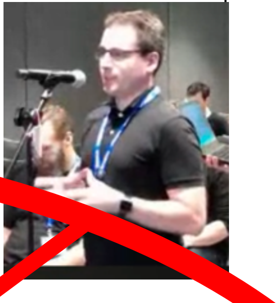
Unique identifier for replay checking

Only valid for a limited time window relative to creation time

Other stuff *could* go here

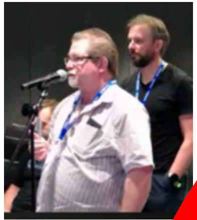


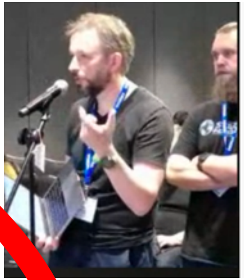


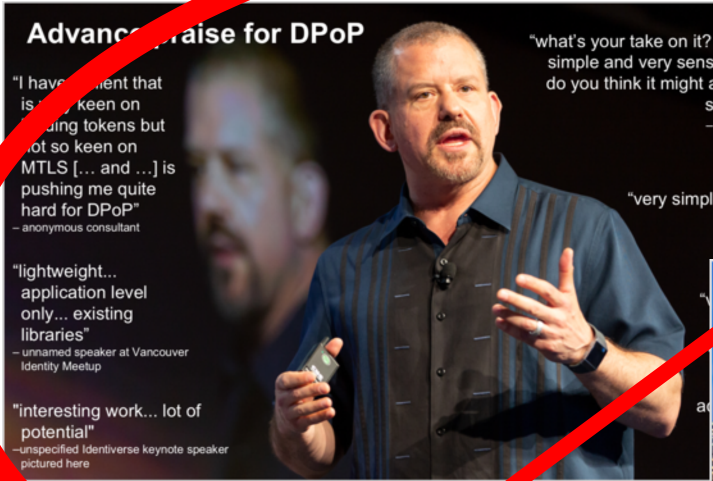


DEUTSCHEPOP
Ausbildung & Studium

Not Presented







Advanc aise for DPoP

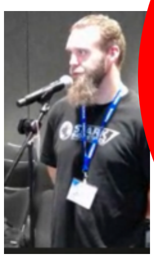
"I have ent that is keen on ing tokens but ot so keen on MTLS [… and …] is pushing me quite hard for DPoP"
– anonymous consultant

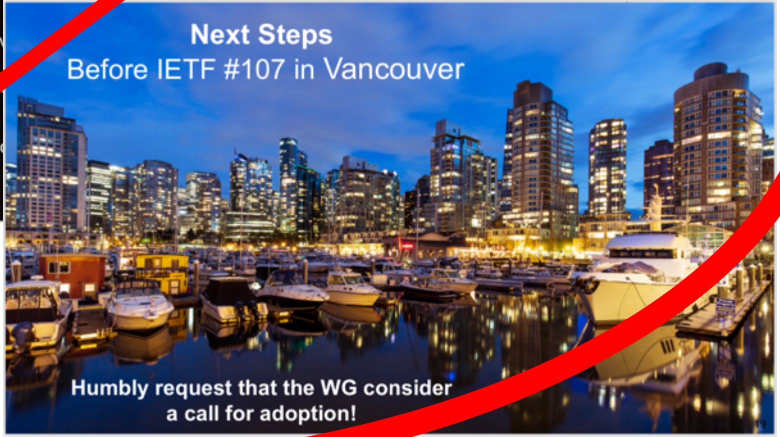
"lightweight… application level only… existing libraries"
– unnamed speaker at Vancouver Identity Meetup

"interesting work… lot of potential"
–unspecified Identiverse keynote speaker pictured here

"what's your take on it? To me it seems simple and very sensible… how soon do you think it might actually turn into something real?"
– anonymous colleague

"very simple, very concise"
– unnamed co-author

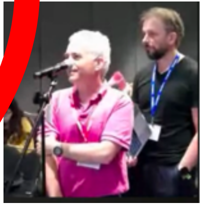


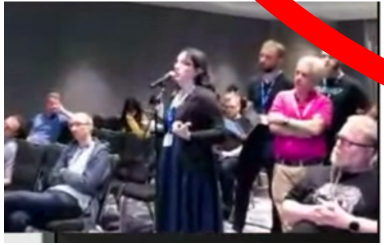


Next Steps

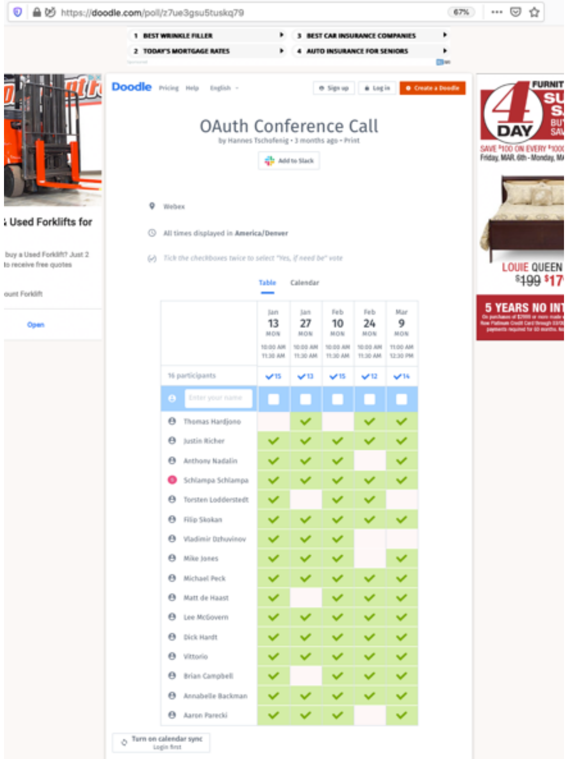
Before IETF #107 in Vancouver

Humbly request that the WG consider a call for adoption!





after the interim is this other interim



https://doodle.com/poll/z7ue3gsu5tuskq79 67%

OAuth Conference Call

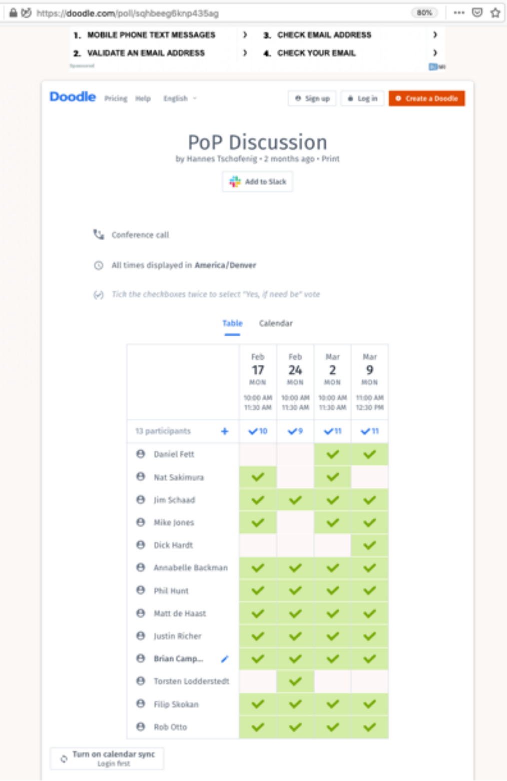
by Hannes Tschofenig • 3 months ago • Print

Webex

All times displayed in **America/Denver**

Tick the checkboxes twice to select "Yes, if need be" vote

	Jan 13 MON 10:00 AM 11:30 AM	Jan 27 MON 10:00 AM 11:30 AM	Feb 10 MON 10:00 AM 11:30 AM	Feb 24 MON 10:00 AM 11:30 AM	Mar 9 MON 11:00 AM 12:30 PM
16 participants	✓15	✓13	✓15	✓12	✓14
Enter your name	□	□	□	□	□
Thomas Hardjono		✓		✓	✓
Justin Richer	✓	✓	✓	✓	✓
Anthony Nadalin	✓	✓	✓		✓
Schlampa Schlampa	✓	✓	✓	✓	✓
Torsten Lodderstedt	✓		✓	✓	
Filip Skokan	✓	✓	✓	✓	✓
Vladimir Dzhuvinov	✓	✓	✓		
Mike Jones	✓	✓	✓		✓
Michael Peck	✓	✓	✓	✓	✓
Matt de Haast	✓		✓	✓	✓
Lee McGovern	✓	✓	✓	✓	✓
Dick Hardt	✓	✓	✓	✓	✓
Vittorio	✓	✓	✓	✓	✓
Brian Campbell	✓		✓	✓	✓
Annabelle Backman	✓	✓	✓	✓	✓
Aaron Parecki	✓	✓	✓		✓



https://doodle.com/poll/sqhbeeg6knp435ag 80%

PoP Discussion

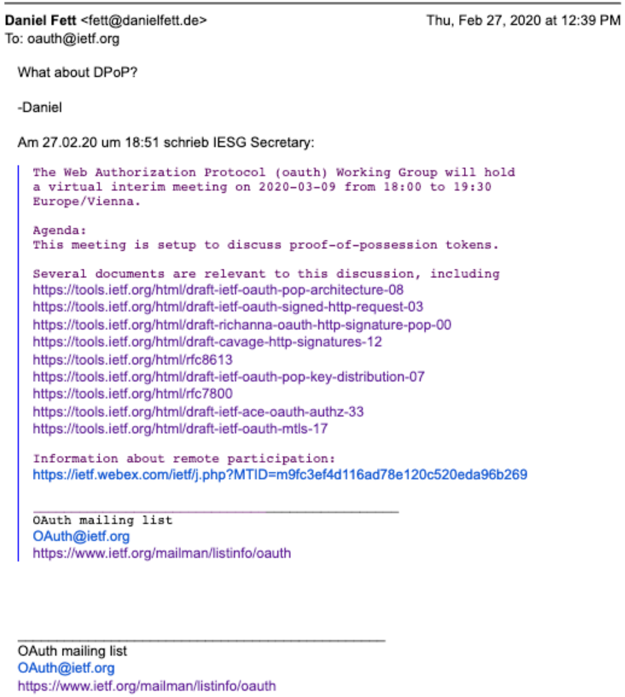
by Hannes Tschofenig • 2 months ago • Print

Conference call

All times displayed in **America/Denver**

Tick the checkboxes twice to select "Yes, if need be" vote

	Feb 17 MON 10:00 AM 11:30 AM	Feb 24 MON 10:00 AM 11:30 AM	Mar 2 MON 10:00 AM 11:30 AM	Mar 9 MON 11:00 AM 12:30 PM
13 participants +	✓10	✓9	✓11	✓11
Daniel Fett			✓	✓
Nat Sakimura	✓		✓	
Jim Schaad	✓	✓	✓	✓
Mike Jones	✓		✓	✓
Dick Hardt				✓
Annabelle Backman	✓	✓	✓	✓
Phil Hunt	✓	✓	✓	✓
Matt de Haast	✓	✓	✓	✓
Justin Richer	✓	✓	✓	✓
Brian Camp...	✓	✓	✓	✓
Torsten Lodderstedt		✓		
Filip Skokan	✓	✓	✓	✓
Rob Otto	✓	✓	✓	✓



Daniel Fett <fett@danielfett.de> Thu, Feb 27, 2020 at 12:39 PM
To: oauth@ietf.org

What about DPoP?

-Daniel

Am 27.02.20 um 18:51 schrieb IESG Secretary:

> The Web Authorization Protocol (oauth) Working Group will hold
> a virtual interim meeting on 2020-03-09 from 18:00 to 19:30
> Europe/Vienna.
>
> Agenda:
> This meeting is setup to discuss proof-of-possession tokens.
>
> Several documents are relevant to this discussion, including
> https://tools.ietf.org/html/draft-ietf-oauth-pop-architecture-08
> https://tools.ietf.org/html/draft-ietf-oauth-signed-http-request-03
> https://tools.ietf.org/html/draft-richanna-oauth-http-signature-pop-00
> https://tools.ietf.org/html/draft-cavage-http-signatures-12
> https://tools.ietf.org/html/rfc8613
> https://tools.ietf.org/html/draft-ietf-oauth-pop-key-distribution-07
> https://tools.ietf.org/html/rfc7800
> https://tools.ietf.org/html/draft-ietf-ace-oauth-authz-33
> https://tools.ietf.org/html/draft-ietf-oauth-mtls-17
>
> Information about remote participation:
> https://ietf.webex.com/ietf/j.php?MTID=m9fc3ef4d116ad78e120c520eda96b269
>
> ____
> OAuth mailing list
> OAuth@ietf.org
> https://www.ietf.org/mailman/listinfo/oauth

____
OAuth mailing list
OAuth@ietf.org
https://www.ietf.org/mailman/listinfo/oauth

[Some] Motivations for [D]PoP

- Do something that's better than bearer
- OAuth 2.0 Security BCP (somewhat aspirationally) recommends use of "sender-constrained" tokens as do various FAPI profiles
  - To prevent token (re)play at a different endpoint/resource (among other benefits)
- Proof-of-possession bound refresh tokens for public clients (also per Security BCP)
- Yet OAuth lacks suitable and widely-applicable PoP mechanism
  - MTLS is "Virtually undeployable [for] general purpose applications" – a WG participant
  - What else is there really?
- Especially lacking for Single Page Applications (SPA)
  - MTLS for OAuth 2.0 would have major UX issues with SPAs
  - Token Binding is dead in the water & needed fetch() API changes anyway

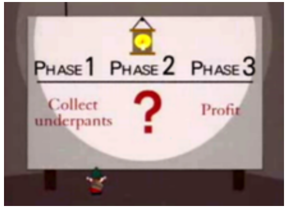
Some existing PoP efforts:

- **OAuth 1.0a** - RFC 5849
- **The OAuth 2.0 Authorization Framework –** RFC 6749
- **OAuth 2.0 Message Authentication Code (MAC) Tokens** - draft-ietf-oauth-v2-http-mac
- **Proof-of-Possession Key Semantics for JSON Web Tokens** – RFC 7800
- **OAuth 2.0 Proof-of-Possession (PoP) Security Architecture** - draft-ietf-oauth-pop-architecture
- **OAuth 2.0 Proof-of-Possession: Authorization Server to Client Key Distribution -** draft-ietf-oauth-pop-key-distribution
- **A Method for Signing HTTP Requests for OAuth** – draft-ietf-oauth-signed-http-request
- **OAuth 2.0 Token Binding** - draft-ietf-oauth-token-binding
- **The OAuth 2.0 Authorization Framework: JWT Pop Token Usage -** draft-sakimura-oauth-jpop
- **OAuth 2.0 Mutual-TLS Client Authentication and Certificate-Bound Access Tokens** – RFC 8705
- **OAuth 2.0 Demonstration of Proof-of-Possession at the Application Layer (DPoP)** - draft-fett-oauth-dpop
- "*a tentative suggestion for an alternative (to/in DPoP) design*" – Neil Madden email
- **Proof-of-Possession Tokens for OAuth Using JWS HTTP Signatures** - draft-richanna-oauth-http-signature-pop
- **Signing HTTP Requests via JSON Web Signatures** - draft-richanna-http-jwt-signature
- **Signing HTTP Messages -** draft-richanna-http-message-signatures formerly draft-cavage-http-signatures

Criticisms of DPoP (paraphrased)

- It’s not draft-ietf-oauth-pop-key-distribution
- An asymmetric crypto operation on every single HTTP request is too expensive
- Tracking `jti` is prohibitive at scale
- Bit of a Rorschach Test even amongst its supporters

Where to now?



- Stay the course
  - Something between doing nothing and -pop-key-distribution + some HTTP signing
- Push forward and adopt and tweak DPoP
  - "… for us mere mortals, DPoP is fine as-is"
  - "we need to sender constrain refresh tokens issued to SPAs yesterday."
- Work toward an approach that's similar(ish) to DPoP using asymmetric keys but with ECDH to amortize the cost of asymmetric crypto over *many* requests (riffing on Neil's idea)
  - allowing for the aggreged/derived key (unique to client/RS or client/AS) to be non-exportable
- ? -> Profit

Gratuitous closing slide featuring the city where will meet together next *

IETF 107 @
Vancouver
Hyatt
Regency

* Some of us anyway pending governmental pandemic response intervention