Alex Davidson, Cloudflare

alex.davidson92@gmail.com

Privacy Pass

Standardizing Anonymous Authorization for the Internet

ACAS20, 2020-08-15

Protocol framework

Privacy Pass

A **performant** protocol framework designed for providing **anonymous**, **authorization tokens** on the **Internet**.

Servers **issue** tokens to clients.

Clients **redeem** tokens for authorization.

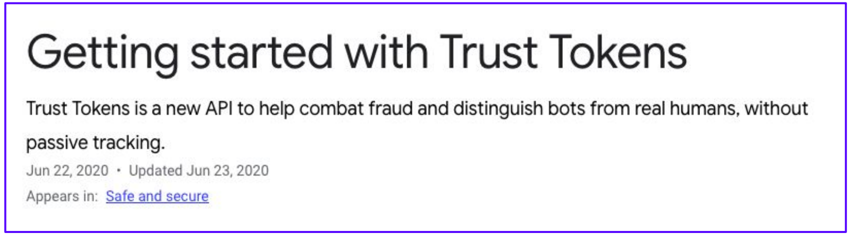
Security guarantees

Anonymity: Redemption event is **unlinkable** to any token issued under the same key.

Unforgeability: Client **cannot** create more valid tokens than it has received.

Applications

Tokens function as lightweight credentials.

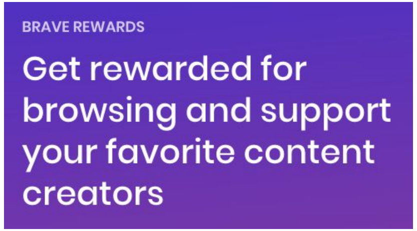


Getting started with Trust Tokens

Trust Tokens is a new API to help combat fraud and distinguish bots from real humans, without passive tracking.

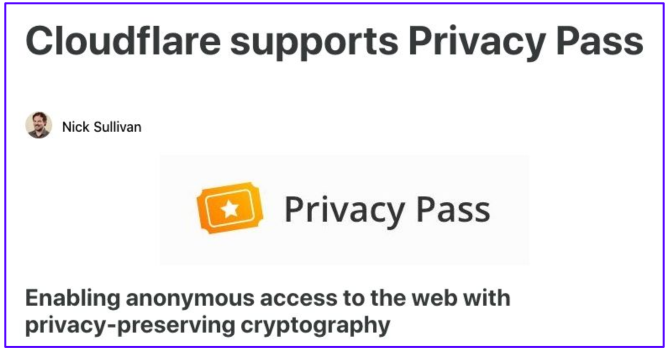
Jun 22, 2020 • Updated Jun 23, 2020

Appears in: Safe and secure



BRAVE REWARDS

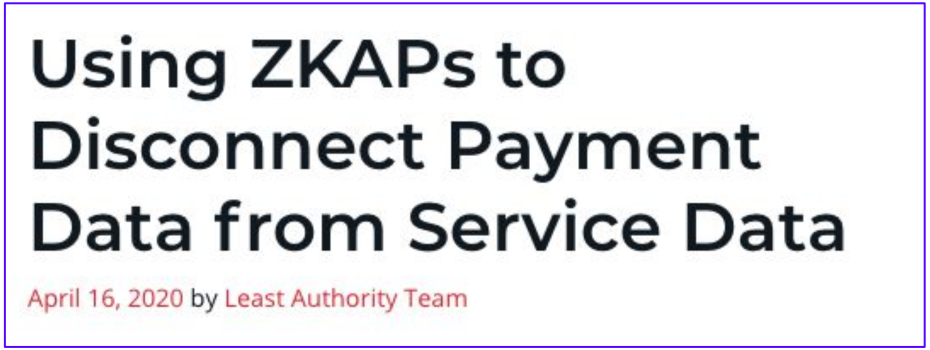
Get rewarded for browsing and support your favorite content creators



Cloudflare supports Privacy Pass

Nick Sullivan

Enabling anonymous access to the web with privacy-preserving cryptography



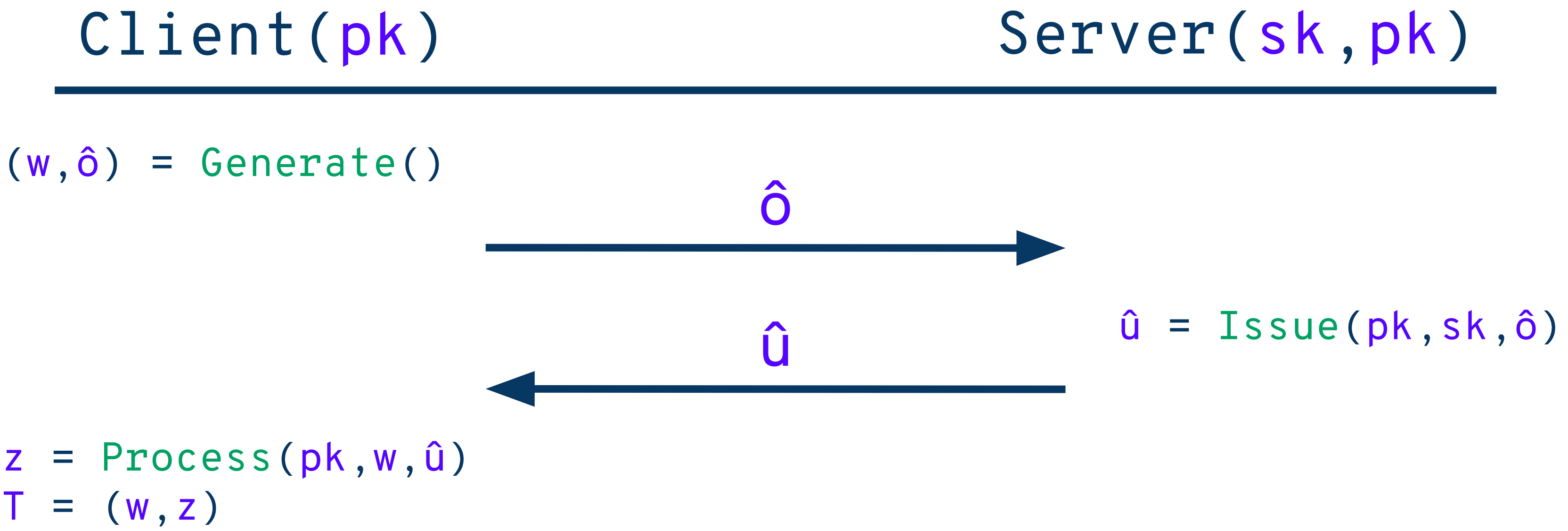
Using ZKAPs to Disconnect Payment Data from Service Data

April 16, 2020 by Least Authority Team

Issuance

Setup: Client retrieves Server's public key pk.

Goal: Client is issued a token T.



Client(pk)

Server(sk,pk)

(w,ô) = Generate()

ô

û

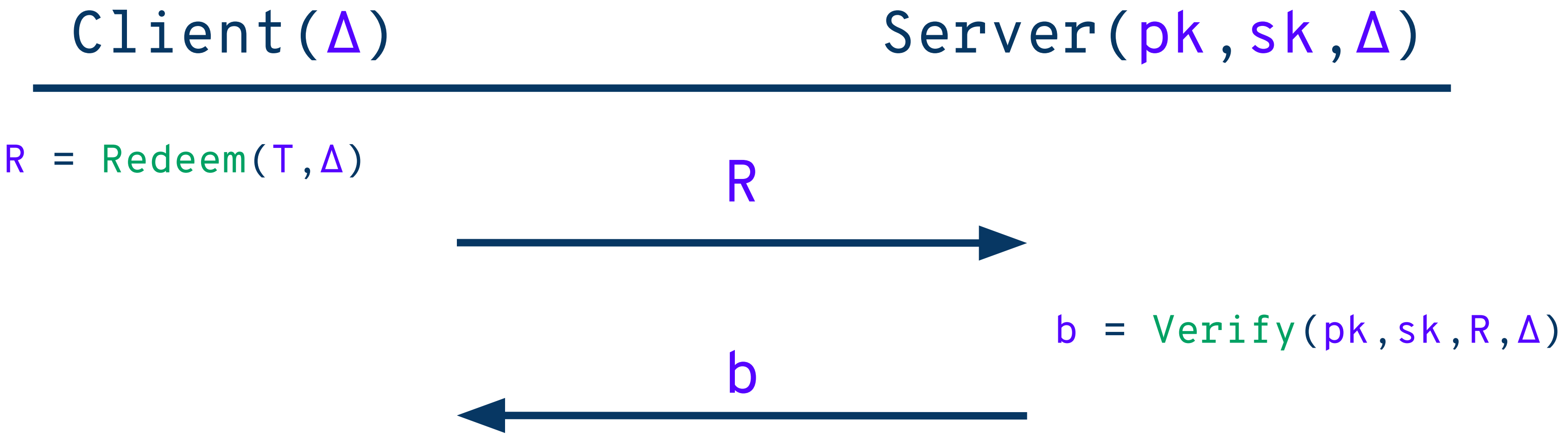
û = Issue(pk,sk,ô)

z = Process(pk,w,û)

T = (w,z)

Redemption

Goal: Server validates the Client token T.



Client(Δ)

Server(pk,sk,Δ)

R = Redeem(T,Δ)

R

b = Verify(pk,sk,R,Δ)

b

Current instantiations

From **Verifiable Oblivious PRFs** (VOPRFs):

- draft-irtf-cfrg-voprf-04
- Allows **symmetric** verification of tokens.

Future instantiations

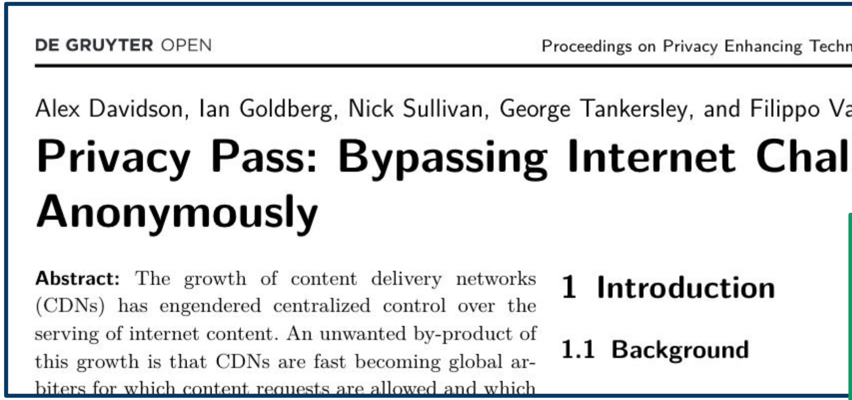
From **VOPRF-related** protocols:

- https://eprint.iacr.org/2020/072
- Symmetric verification + private **metadata**.

From **blind signature schemes**:

- As yet unspecified (open problem)
- Allows **public** verification of tokens.

Security proofs



DE GRUYTER OPEN

Proceedings on Privacy Enhancing Technologies ; 2018 (3):164–180

Alex Davidson, Ian Goldberg, Nick Sullivan, George Tankersley, and Filippo Valsorda

Privacy Pass: Bypassing Internet Challenges Anonymously

Abstract: The growth of content delivery networks (CDNs) has engendered centralized control over the serving of internet content. An unwanted by-product of this growth is that CDNs are fast becoming global arbiters for which content requests are allowed and which

1 Introduction

1.1 Background

popets-2018-0026

Efficient Anonymous Tokens with Private Metadata Bit

Ben Kreuter[1], Tancrède Lepoint[1], Michele Orrù[2,3,4], and Mariana Raykova[1]

[1] Google, {benkreuter,tancrede,marianar}@google.com
[2] École Normale Supérieure, CNRS, PSL University, Paris, France, michele.orru@ens.fr
[3] Inria, Paris, France
[4] Recurse Center, New York, USA

eprint.iacr.org/2020/072

Internet standardization

Internet Engineering Task Force (IETF)

IETF®

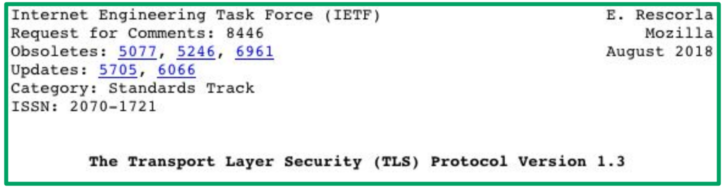
TLS

ACME

QUIC

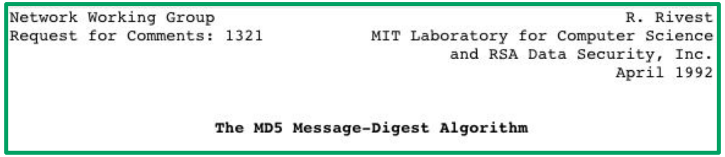
Working groups

RFCs



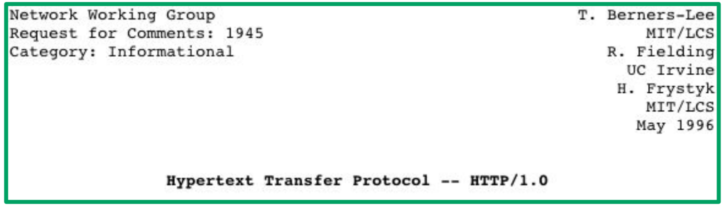
```
Internet Engineering Task Force (IETF)                       E. Rescorla
Request for Comments: 8446                                       Mozilla
Obsoletes: 5077, 5246, 6961                                  August 2018
Updates: 5705, 6066
Category: Standards Track
ISSN: 2070-1721


        The Transport Layer Security (TLS) Protocol Version 1.3
```



```
Network Working Group                                          R. Rivest
Request for Comments: 1321           MIT Laboratory for Computer Science
                                             and RSA Data Security, Inc.
                                                              April 1992


                 The MD5 Message-Digest Algorithm
```



```
Network Working Group                                     T. Berners-Lee
Request for Comments: 1945                                       MIT/LCS
Category: Informational                                       R. Fielding
                                                               UC Irvine
                                                              H. Frystyk
                                                                 MIT/LCS
                                                                May 1996


                Hypertext Transfer Protocol -- HTTP/1.0
```

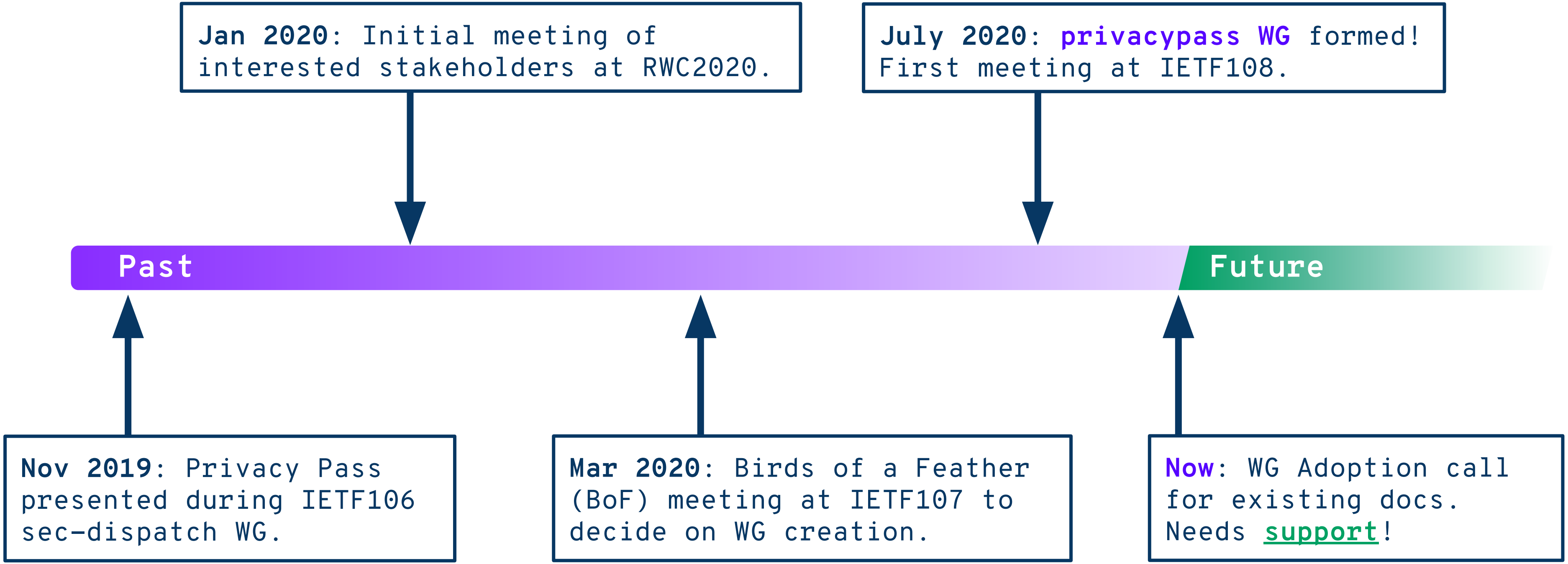
ACAS20, 2020-08-15

Goals for Privacy Pass

Standardization of:

- Protocol **design** and security guarantees.
- Application architecture and privacy-preserving **ecosystem**.
- Application-layer integration.

Progress timeline



Nov 2019: Privacy Pass presented during IETF106 sec-dispatch WG.

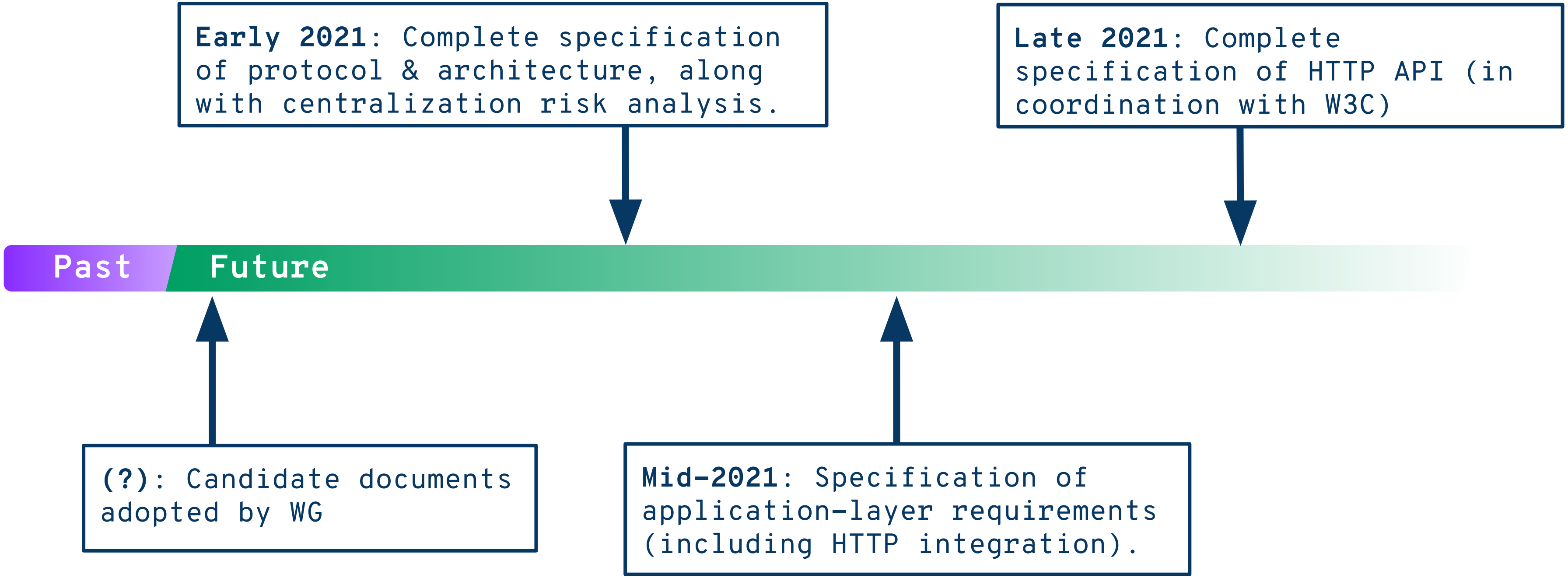
Jan 2020: Initial meeting of interested stakeholders at RWC2020.

Mar 2020: Birds of a Feather (BoF) meeting at IETF107 to decide on WG creation.

July 2020: **privacypass WG** formed! First meeting at IETF108.

Now: WG Adoption call for existing docs. Needs support!

Progress timeline



(?): Candidate documents adopted by WG

Early 2021: Complete specification of protocol & architecture, along with centralization risk analysis.

Mid-2021: Specification of application-layer requirements (including HTTP integration).

Late 2021: Complete specification of HTTP API (in coordination with W3C)

Existing documents

Charter: charter-ietf-privacypass

Drafts:

- draft-davidson-pp-protocol
- draft-davidson-pp-architecture
- draft-svaldez-pp-http-api

GitHub: alxdavids/privacy-pass-ietf/

Current open questions

- Technical protocol specifications using new underlying primitives.
- How do we identify (& audit) malicious servers?
- Privacy leakage tolerance.
- Key management requirements.

How can you help?

The WG is open for **all** to join and contribute!

- Join the mailing list discussion.
- Read the documents.
- Work on open issues in GitHub.
- Write, edit & review.

Alex Davidson, Cloudflare

alex.davidson92@gmail.com

Privacy Pass

Standardizing Anonymous Authorization for the Internet

ACAS20, 2020-08-15