A LIGHTWEIGHT ZERO-KNOWLEDGE PROTOCOL
WOULDN’T IT BE NICE TO HAVE AN ONLINE EQUIVALENT TO CASH?

Desirable properties

- Withdrawals and transactions are un-linkable
- Can only be created by a central authority
- Performant at Internet scale
Serial Number: 00003304043030
Legal Tender
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 are blocked in an attempt to stanch malicious traffic. In particular, in some cases honest users — especially those behind shared IP addresses, including users of privacy tools such as Tor, VPNs, and I2P — can be unfairly targeted by attempted ‘catch-all solutions’ that assume these users are acting maliciously. In this work, we provide a solution to prevent users from being exposed to a disproportionate amount of internet challenges such as CAPTCHAs. These challenges are at the very least an-

1 Introduction

1.1 Background

An increasingly common trend for websites with globally high visitation is to use content delivery networks (CDNs) to host or cache their resources. According to Cisco, CDNs will serve 71% of all traffic in 2021, up from 52% in 2016 [7]. Some of the most well-known CDNs include Akamai, Cloudflare, Fastly, and Amazon Cloudfront. These CDNs typically house data centers across the globe, meaning that access to websites is sped up by serving from locations geographically near requests.

On top of this, CDNs usually offer protection ser
A CAPTCHA SOLUTION

First CAPTCHA

Token → Blind Token → Solve CAPTCHA, Blind Token

Signature ← Blind Signature ← Blind Signature, Bypass, Cookie

Second CAPTCHA

Token ← Signature ← Bypass, Cookie

Validate → CAPTCHA Public Key

CAPTCHA Private Key
BLINDED RSA: PUBLICLY VERIFIABLE
PRIVACY PASS

VOPRF: VERIFIABLE ONLY BY THE ISSUER
 PRIVACY PASS

RUNNING CODE

- Firefox and Chrome extension
- ~135,000 active users
- 500K redemptions per week
- All Cloudflare sites
PRIVACY PASS

MORE USE CASES

Chromium Blog
News and developments from the open source browser project

Potential uses for the Privacy Sandbox
Thursday, August 22, 2019

PRIVATE STORAGE
a joint venture product developed and maintained by:

The Path from S4 to PrivateStorage

brave / brave-browser

Security and privacy model for ad confirmations
mandar-brave edited this page on Mar 8 - 7 revisions

Application

Parties
- Users running Brave browser
- Advertisers
- Brave operators

Fighting fraud using partially blind signatures
The Privacy Pass Protocol

draft-privacy-pass-00

Abstract

This document specifies the Privacy Pass protocol for anonymously authorizing clients with services on the Internet.
WHAT IS THE SCOPE OF THE WORK TO BE DONE?

▸ Basic Privacy Pass protocol, HTTP headers, VOPRF integration

▸ Extensibility to support features specific to the use cases listed

▸ A mini-working group sized amount of work?
Several applications have the need for a mechanism to be able to issue and redeem anonymous tokens with the following properties:

- Tokens are issued in groups (groups form anonymity sets)
- An issued token can be confirmed to be part of a specific group
- The verifier of a token cannot link that token to a specific issuance, only its group
The primary goal of this working group is to:

- Specify a protocol that provides the mechanism listed above with the required security properties
- Specify the use of this protocol in an HTTPS setting
- It is not a goal to enable interoperability/federation of multiple token issuers
- (TBD) Define a way to embed a small amount of metadata into a token that is only known to the issuer
PRIVACY PASS

NICK SULLIVAN
CLOUDFLARE
@GRITTYGREASE