DISPATCH
@IETF122

draft-darling-key-directory-over-http

https://datatracker.ietf.org/doc/draft-darling-key-directory-over-http

Fisher Darling, Thibault Meunier, Simon Newton (Cloudflare)

IETF

Motivation

Multiple protocols rely on public key cryptography
Some encourage distribution of their keys via HTTP
JOSE, COSE, DAP, Privacy Pass, OHTTP, [your-protocol-here]

They all have different levels of details regarding implementation:

- *How does the protocol interact with HTTP cache*
- *How does it work with HTTP when keys are rotated*
- *How do clients discover an endpoint to retrieve keys*
- *How to ensure my directory is consistent for all clients*

This document aims to provide recommendations for existing and future protocols.

Background

RFC 9205 Building protocols with HTTP
Best current practice to write protocols that use HTTP (June 2022)

RFC 7517 JSON Web Key
Section 6 defines a Key Directory (Key Set)
OpenID Connect Core
Identity layer for OAuth 2.0. Leverages JOSE

RFC 9578 Privacy Pass Issuance Protocols
Section 4 defines a Key Directory
Privacy Pass Mirrors Checking Resource Consistency with HTTP Mirrors
This is an example where recommendations would help

Format is out of scope. Use base64, JWK, COSE.
This is up to protocol implementers

IETF

Background

A discussion has started within SPICE, and on GitHub about the scope

The draft spans across multiple areas: CFRG, JOSE, COSE, SPICE, HTTPAPI, PRIVACYPASS, KEYTRANS, ...

Non exhaustive formatted list https://key-directory-over-http.research.cloudflare.com/

IETF

Hoped-for dispatch outcome

*Direct the work to **an existing WG***

Leverage current expertise in building HTTP API and distributing public cryptographic key material over HTTP.

*Propose **a new focused WG***

Have a dedicated place with more participant.

*Preferred option: **an existing WG***

IETF