Oblivious HTTP

draft-ietf-ohai-oblivious-http

Thomson, Wood — IETF 114 — OHAI
Updates

Date-based anti-replay mitigation merged

Improved text on differential treatment (shadow banning as a use case)

Terminology and editorial updates

Key schedule change (details follow)
Old Key Schedule
Request Encapsulation

Client Functionality

- Public Key
- "ohttp/req"
- Binary Request
- HPKE
- AEAD
- Encapsulated Request
- OHTTP Config Parameters
- Exported Key

Gateway Functionality

- Private Key
- "ohttp/req"
- Encapsulated Request
- HPKE
- AEAD
- Exported Key
- Binary Request
- OHTTP Config Parameters

Key is not bound to OHTTP config params
Old Key Schedule
Response Encryption

Gateway Functionality

Client Functionality

Exported Key

AEAD

Encapsulated Response

Binary Response

“ohttp/resp”

Encapsulated Response

Binary Response

“ohttp/resp”

Cipheredtext is not bound to OHTTP config params
New Key Schedule
Request Encryption

Client Functionality

Gateway Functionality

Public Key

Private Key

“ohttp/req” + OHTTP Config Parameters

Binary Request

AEAD

Exported Key

Encapsulated Request

Exported Key

Encapsulated Request

Key is bound to OHTTP config params!
Request Date

Request-Date I-D is somewhat stalled, yet OHTTP normatively references it.

PR#137 pulls in the relevant pieces into draft-ietf-ohai-obliviou-s-http to unblock forward progress.
Questions?
WGLC?
Oblivious HTTP

draft-ietf-ohai-oblivious-http

Thomson, Wood — IETF 114 — OHAI