

Oblivious HTTP

`draft-ietf-ohai-oblivious-http`

Thomson, Wood — IETF 114 — OHAI

Updates

Date-based anti-replay mitigation merged

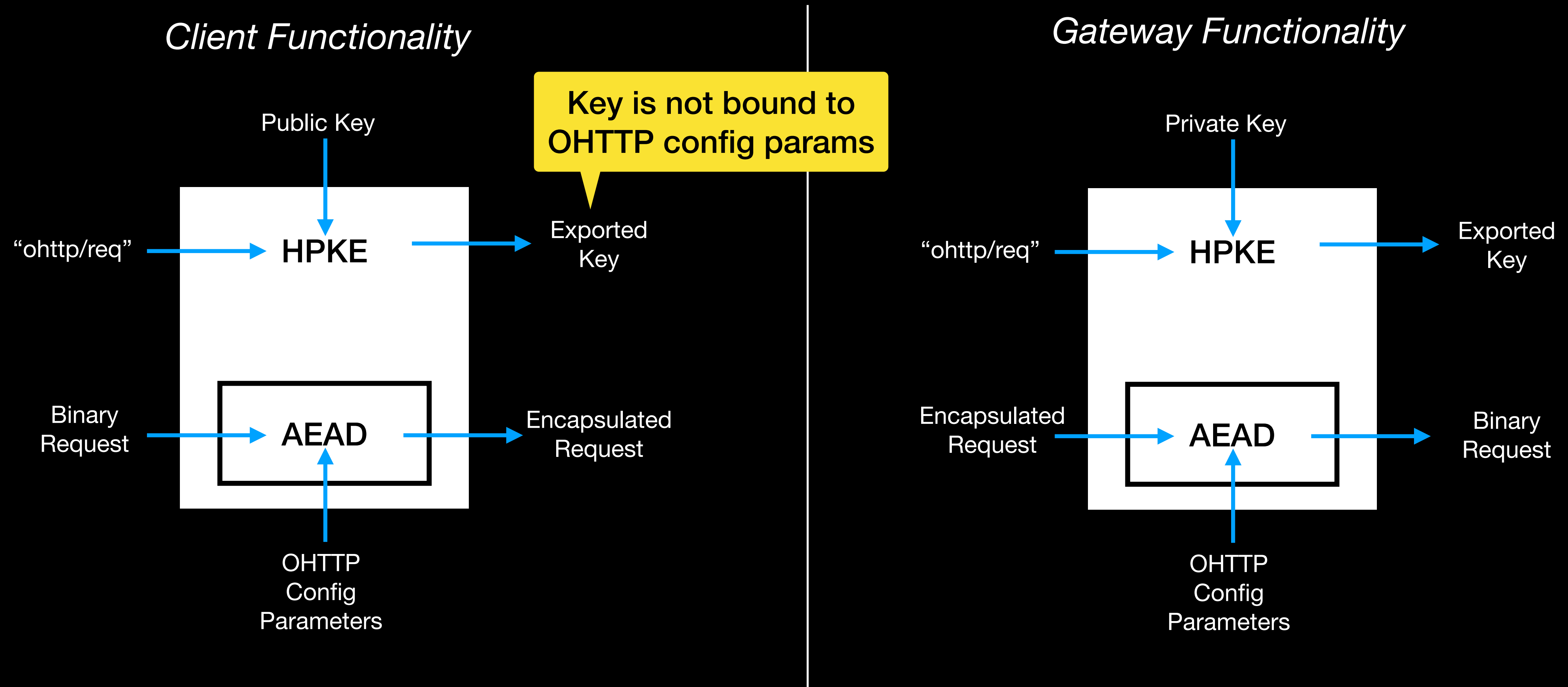
Improved text on differential treatment (shadow banning as a use case)

Terminology and editorial updates

Key schedule change (details follow)

Old Key Schedule

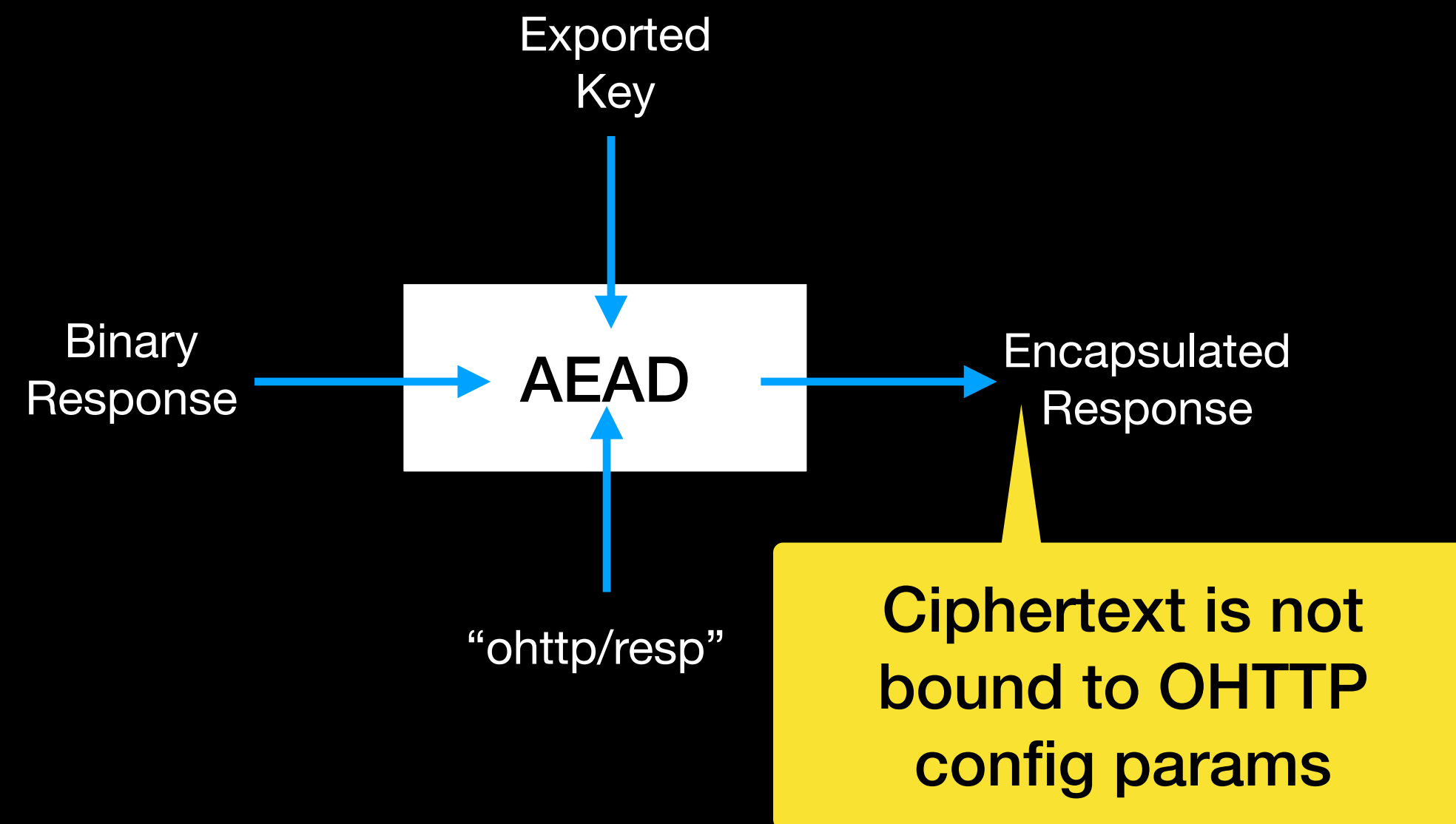
Request Encapsulation



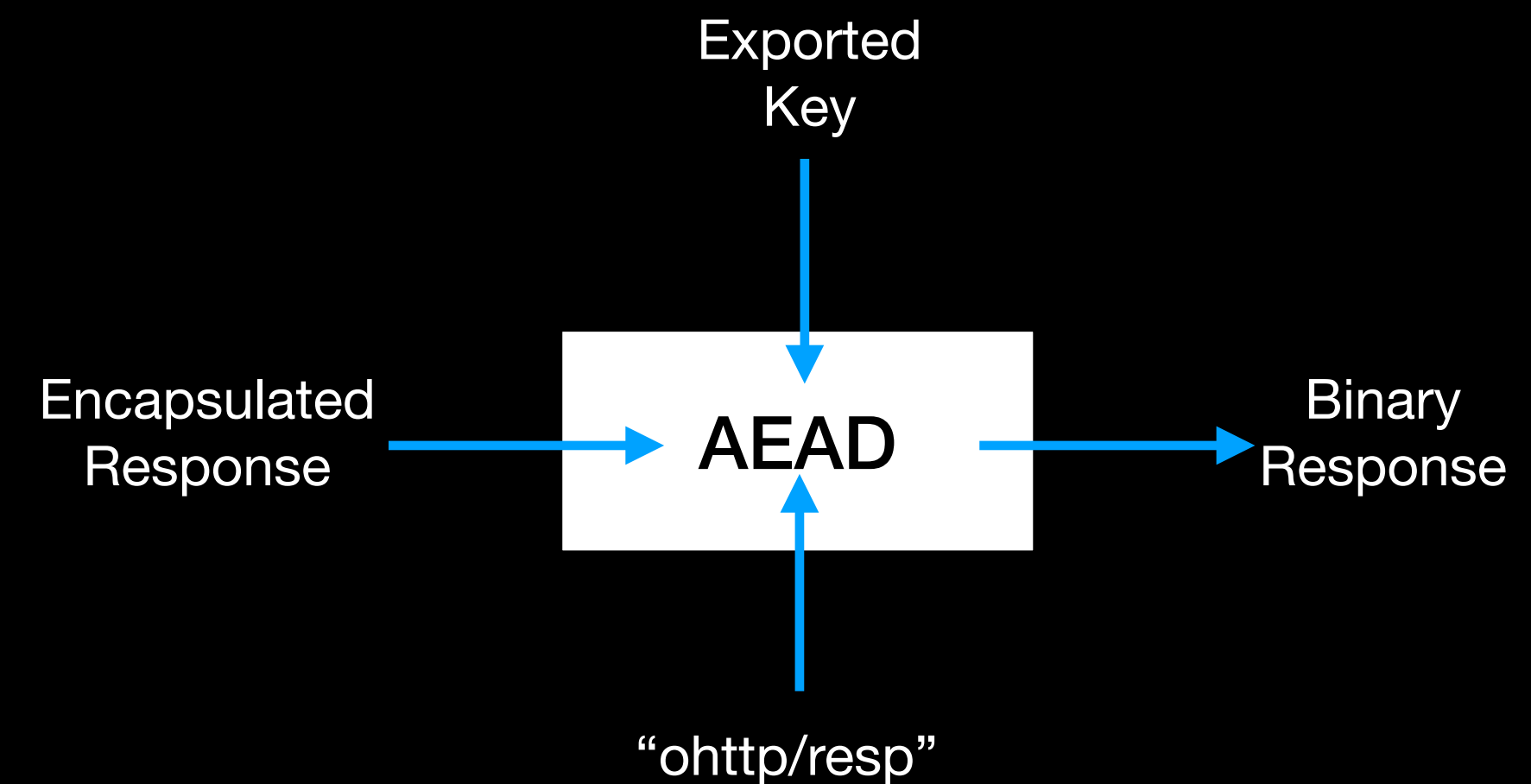
Old Key Schedule

Response Encryption

Gateway Functionality

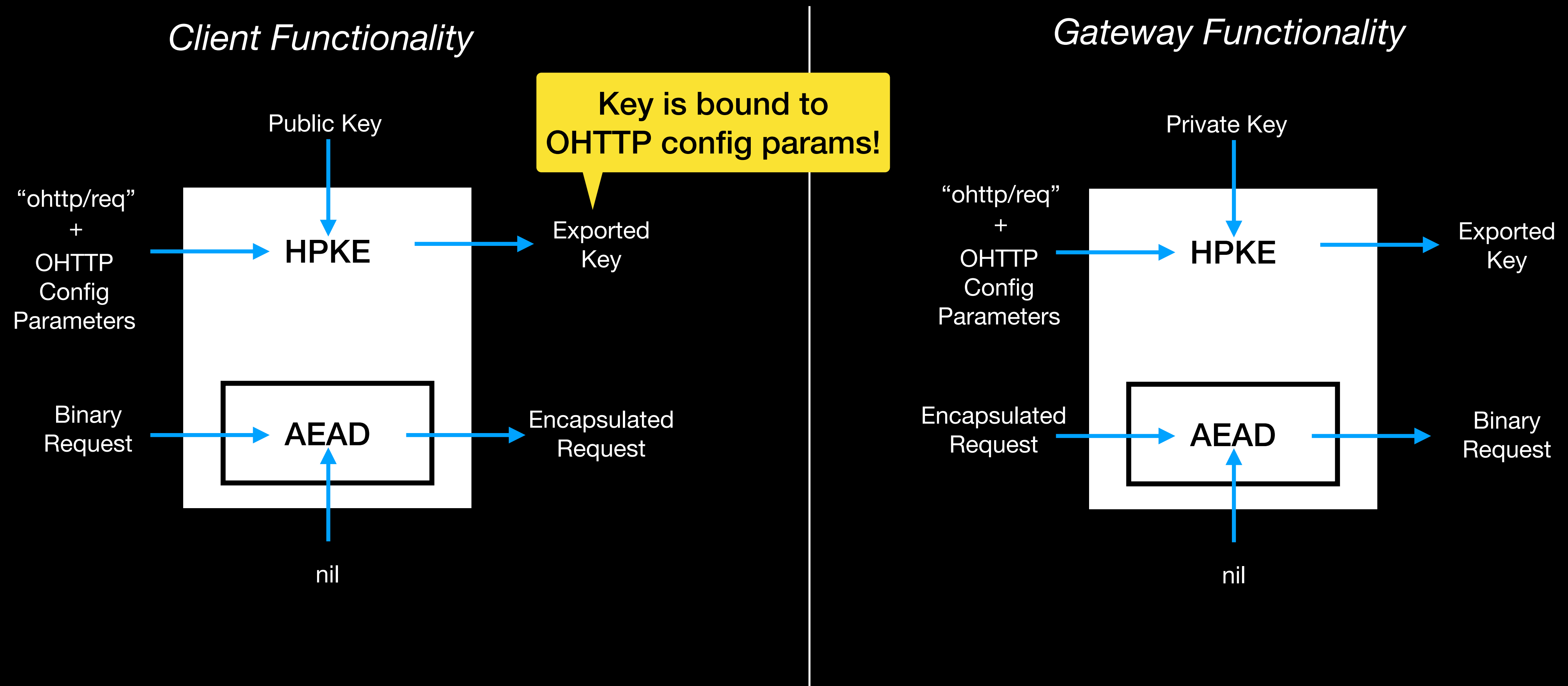


Client Functionality



New Key Schedule

Request Encryption



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-oblivious-http to unblock forward progress

Questions?
WGLC?

Oblivious HTTP

`draft-ietf-ohai-oblivious-http`

Thomson, Wood — IETF 114 — OHAI