

Attestable HTTP (**HTTPPA**)

Shih-Han (Hans) Wang, Gordon King, Nick Li, Ned Smith, Krzysztof Sandowicz

<https://datatracker.ietf.org/doc/html/draft-sandowicz-httpbis-httpa2-01.txt>

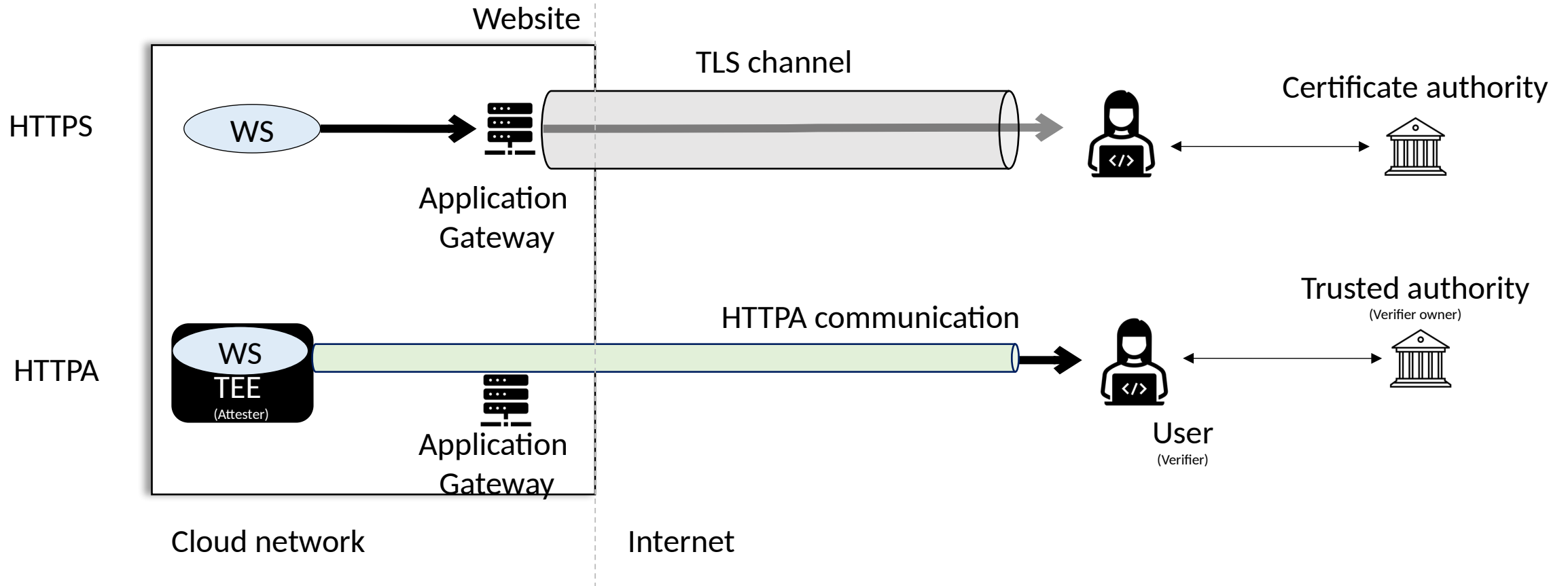
What is Attestable HTTP?

- HTTP extensions for binding remote attestation messages to HTTP headers.
 - Secure communication enables end-to-end message protection to TEE endpoints.
 - L7 protection establishes trusted communication for web services running inside a TEE.
 - However, HTTPPA is not specific to TEE endpoints.
- We are proposing extending HTTP with an 'ATTEST' method and a set of 'Attest-*' headers for standardization.
 - Mutual-HTTPPA to build L7 trusted end-to-end communication.
- Achieve trustworthy web services.

Background

- There is customer demand for a wide range of secure web services.
- Web services are mostly not attested.
- TEE is an emerging technology that protects data in use and is a reasonable endpoint for HTTP message exchanges.
- There is a need for remote attestation at the HTTP layer.

HTTPPA vs. HTTPS



Where do we go?

- Dispatch?
 - HTTPBIS?
 - Other?
- SecDispatch?
 - RATS? TEEP?
 - Other?