The Signature HTTP Authentication Scheme

(fka HTTP Unprompted Authentication)

draft-ietf-httpbis-unprompted-auth

IETF 118 – Prague – 2023-11-09

David Schinazi – dschinazi.ietf@gmail.com
David Oliver – david@guardianproject.info
Jonathan Hoyland – jonathan.hoyland@gmail.com

Quick Summary, Motivation, History

Client authenticates to server

Using asymmetric cryptography

Server hides the fact that it serves authenticated resources

Adopted by HTTPBIS in February, discussed in Yokohama in March

Changed almost everything between Yokohama and San Francisco

A few more tweaks since but now things are settling

Rough Shape of Solution

Use TLS Key exporter to generate nonce

Sign the nonce

Doesn't leak any information

Can't be replayed on a separate connection

Exported Authenticators – RFC 9261 (#2604)

Taking a TLS key exporter and signing stuff? Sounds familiar

Did some work considering what it would take to rebuild on top of EA

While it was mechanically feasible

It would require some tweaks to TLS

And would be much harder to implement outside of TLS stacks

So we landed on keeping Unprompted Auth separate from EA

TLS Exporter Context

Signature Algorithm

Key ID

Public Key

Origin (Scheme, Host, Port)

Realm

Authentication Parameters

Key ID

Public Key

Signature

Signature Algorithm

Verification (portion of key exporter output)

Security Analysis

Tamarin Model

Analysis redone with "Seems Legit" in mind

Security bound matches the one from SIGMA

Moar security always B moar good, halp B welc0m3

Implementation

One complete implementation of an earlier draft

Working on independent implementations of latest draft

Next Steps

Want to get some implementation experience before WGLC

Assuming implementation work doesn't find surprises,

Aim to get to WGLC before Brisbane?

The Signature HTTP Authentication Scheme

(fka HTTP Unprompted Authentication)

draft-ietf-httpbis-unprompted-auth

IETF 118 – Prague – 2023-11-09

David Schinazi – dschinazi.ietf@gmail.com
David Oliver – david@guardianproject.info
Jonathan Hoyland – jonathan.hoyland@gmail.com