The Signature HTTP Authentication Scheme
(fka HTTP Unprompted Authentication)

draft-ietf-httpbis-unprompted-auth

IETF 119 – Brisbane – 2024-03-19

David Schinazi – dschinazi.ietf@gmail.com
David Oliver – david@guardianproject.info
Jonathan Hoyland – jonathan.hoyland@gmail.com
Quick Summary, Motivation, Mechanism, History

Client authenticates to server using asymmetric cryptography

Server hides the fact that it serves authenticated resources

Leverages a TLS key exporter

Adopted back in February 2023

Closed remaining open issues in Prague
What's new since Prague

- 4 independent open-source implementations that interoperate
  - http-sigauth-java
  - http-signature-auth-go
  - Google QUICHE
  - ngx-http-sig-auth-module

- Security analysis in Tamarin
Oh, one more thing

How to use this with intermediaries?

Today draft recommends intermediary sends key exporter to upstream HTTP server

But how to send it is left as an exercise to the reader

Two implementers have use cases for intermediary support

Proposal: PR#2762 – define a new header field to send it as an SF Byte Sequence

Signature/Auth-Context: :VGrpcyBleG...0ZXMgI/+h:
Name Collision

draft-cavage-http-signatures-12

Replaced by RFC 9421 (HTTP Message Signatures)

But implemented and deployed

Solution: rename the HTTP auth scheme
Renaming the auth scheme

Authorization: UnpromptedSignature
Next Steps

Editors would like to perform a quick editorial pass

Then perhaps WGLC?
The Signature HTTP Authentication Scheme
(fka HTTP Unprompted Authentication)

draft-ietf-httpbis-unprompted-auth

IETF 119 – Brisbane – 2024-03-19

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