

WIMSE IETF-125: HTTP Signatures

Joe Salowey and Yaron Sheffer

...

[draft-ietf-wimse-http-signature-02](#)

Status

One major change in -02, on next slide

In our opinion, ready for WGLC

Audience – The Problem

- We had a discussion about requiring a message receiver to ensure that it is the intended audience for the message
- The latest conclusion is [Sec. 1.3](#) of the Workload Creds draft

- Complexity:
 - The sender may not know the receiver's WIMSE identity
 - Some deployments rewrite URLs, some don't
 - Rewrite can happen on the sender, on the receiver, or a TLS proxy in between

Audience – Proposed Solution

- Sender generates an HTTP message with a Request URI

Audience (some small print applies)

`https://target.com/service/endpoint?param=val`

Authority Request Target

- The previous version only signed *@request-target*
- Version -02 adds a *WIMSE-Audience* HTTP header that must be signed
- Identical to the *aud* claim of the WPT
- Small print: However, there may be some normalization, rewriting or other processes that require the audience to be set to a deployment-specific value.

Thank You!