



Workload Identity Practices

Yaroslav Rosomakho

Arndt Schwenkschuster

Since IETF 124 - Kathleen's review

- Clarify identity vs. credentials
- Explain what federation actually produces
- Consistent terminology across credential types
- Tighten SPIFFE terminology

Since IETF 124 - Joe's review

- Clarify multiple token - each with own audience & lifetime
- Add consequences to security considerations
- Differentiate from Workload Identity Document - next slide



Issue [#69](#): Differentiate Workload Identity Document

- Cloud Providers offer Instance Metadata Endpoints, which issues 2 distinct types of documents:
 - Issues access credentials that can be used to access resources
 - Issues signed instance metadata document that contains metadata (account, region, type, name, etc.)
- Results in 2 distinct flows
 - Access resources -> use access credential
 - Federation -> use signed instance metadata document

Working Group Last Call



Contributors

Benedikt Hofmann, **Hannes** Tschofenig, **Edoardo** Giordano, **Dag** Sneeegen, **Ned** Smith, **Dean** H. Saxe, **Yaron** Sheffer, **Andrii** Deinega, **Marcel** Levy, **Justin** Richer, **Pieter** Kasselmann, **Simon** Canning, **Evan** Gilman, **Joseph** Salowey, **Kathleen** Moriarty and **Flemming** Andreassen.

Other changes since IETF 123 (Madrid)

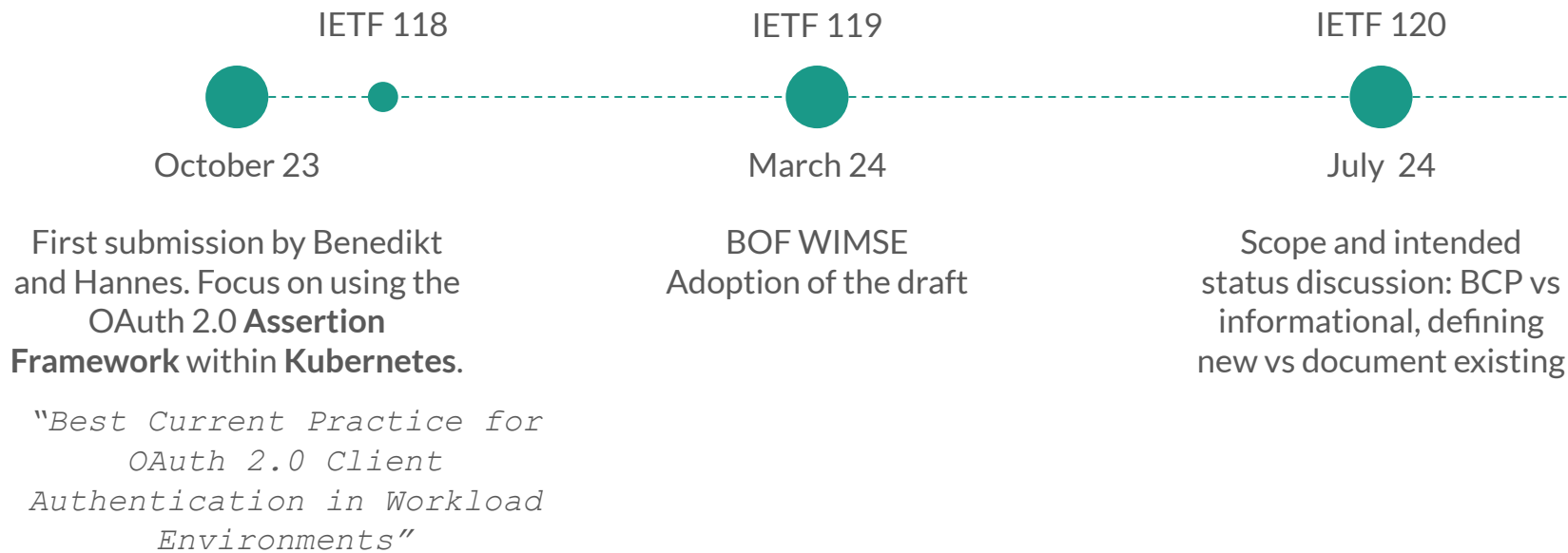
- Add atomicity and flushing requirements to file-system section
- Make it clear that invalidation is a matter of querying the status
- Rework local api section & security considerations
- Refer to RFC 7517 in SPIFFE and add clarity on key distribution
- Editorial changes



WGLC in October



History of the draft





History of the draft - continued

IETF 121



November 24

Added other workload
platforms: Cloud
providers, SPIFFE and
Continuous Deployment
& Delivery

December 24



Change of name & status:
BCP -> Informational

"Workload Identity Practices"

IETF 122



March 25

Added delivery
mechanisms:
Environment variables,
File system & Local
APIs



History of the draft - continued

IETF 123



July 25

WGLC



October 25

IETF 124



November 25

IETF 125



March 26

More generic
“federation” term instead
of OAuth 2.0 specifics
(Assertion framework)