WIMSE

Welcome and Chair Updates

IETF 119, Brisbane
March 18, 2024

This is a reminder of IETF policies in effect on various topics such as patents or code of conduct. It is only meant to point you in the right direction. Exceptions may apply. The IETF's patent policy and the definition of an IETF "contribution" and "participation" are set forth in BCP 79; please read it carefully.

As a reminder:

- By participating in the IETF, you agree to follow IETF processes and policies.
- If you are aware that any IETF contribution is covered by patents or patent applications that are owned or controlled by you or your sponsor, you must disclose that fact, or not participate in the discussion.
- As a participant in or attendee to any IETF activity you acknowledge that written, audio, video, and photographic records of meetings may be made public.
- Personal information that you provide to IETF will be handled in accordance with the IETF Privacy Statement.
- As a participant or attendee, you agree to work respectfully with other participants; please contact the ombudsteam (https://www.ietf.org/contact/ombudsteam/) if you have questions or concerns about this.

Definitive information is in the documents listed below and other IETF BCPs. For advice, please talk to WG chairs or ADs:

- BCP 9 (Internet Standards Process)
- BCP 25 (Working Group processes)
- BCP 25 (Anti-Harassment Procedures)
- BCP 54 (Code of Conduct)
- BCP 78 (Copyright)
- BCP 79 (Patents, Participation)
- https://www.ietf.org/privacy-policy/(Privacy Policy)

Agenda

- **Welcome** - 5 min (chairs)
- **What is WIMSE and Why Are We Here** - 20 min (chairs)
- **Transaction Tokens** - 15 min (George)
- **Identity Chaining** - 15 min (Kelly)
- **Token Delivery BCP** - 10min (Hannes)
- **WIMSE Architecture** - 15 min (Joe)
- **Deliverables Review and Calls for Adoption** - 30 min (chairs)
- **Other Business** - 10min (chairs)

Welcome to WIMSE!

Workload

Identity in

Multi-

System

Environments

We’re a working group now!

HUGE thanks to everyone who contributed
to the chartering discussion and text

Meet Your Chairs: **Justin Richer**

- System architect, software engineer, author
- Involved mostly in the security area of IETF
  - Worked on OAuth, GNAP, HTTP Message Signatures
- Some standards outside of IETF
  - OpenID Connect, UMA, DID, VC
- Previously chaired COSE (v 1.0)
- Consultant with a variety of clients
  - Currently includes Authlete, NIST, SPIRL, UberEther
- Publishes *Cards Against Identity* annually
- Only dressed up for that headshot because they made him put on “a nice shirt”

Meet Your Chairs: **Pieter Kasselman**

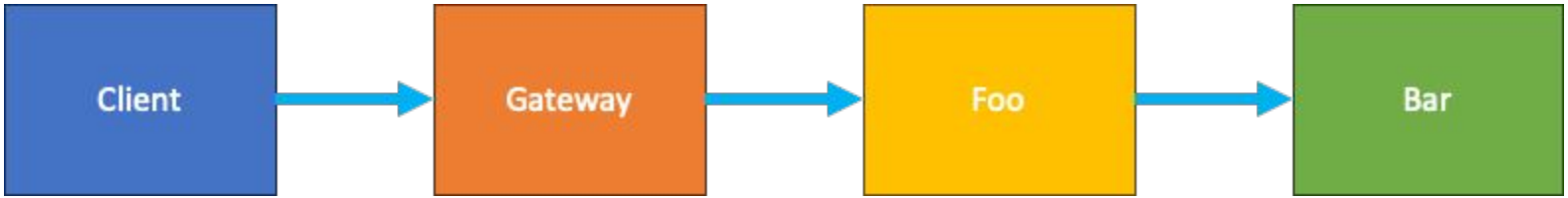
- Identity standards enthusiast
  - Active in IETF OAuth WG
  - Sprinkling of cryptography, biometrics, identity and security
  - Know how to write code, specs and business plans
- Works at Microsoft
  - Windows, Office, Entra
- Area of Focus
  - Securing Workload Identity
- Owns a *Cards Against Identity* pack
- Unprotesting wearer of “nice shirts”


WORKLLOP IDENTIYE FOR MULISICE ENVROICEES
WORKING GLOD GROUP

Now the real work begins!

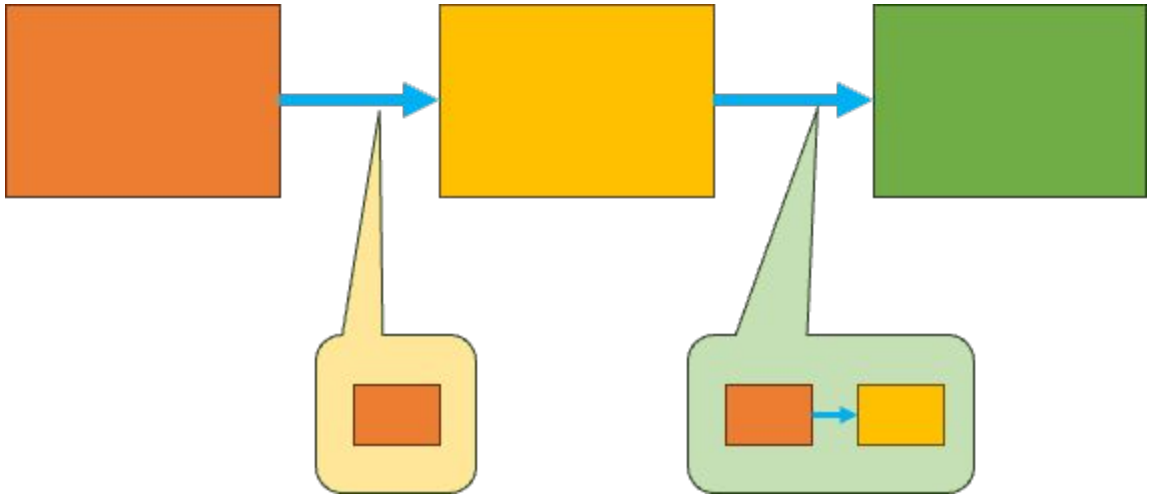
What is a *workload*?

a *running instance* of software executing for a *specific purpose*


Client
Gateway
Foo
Bar

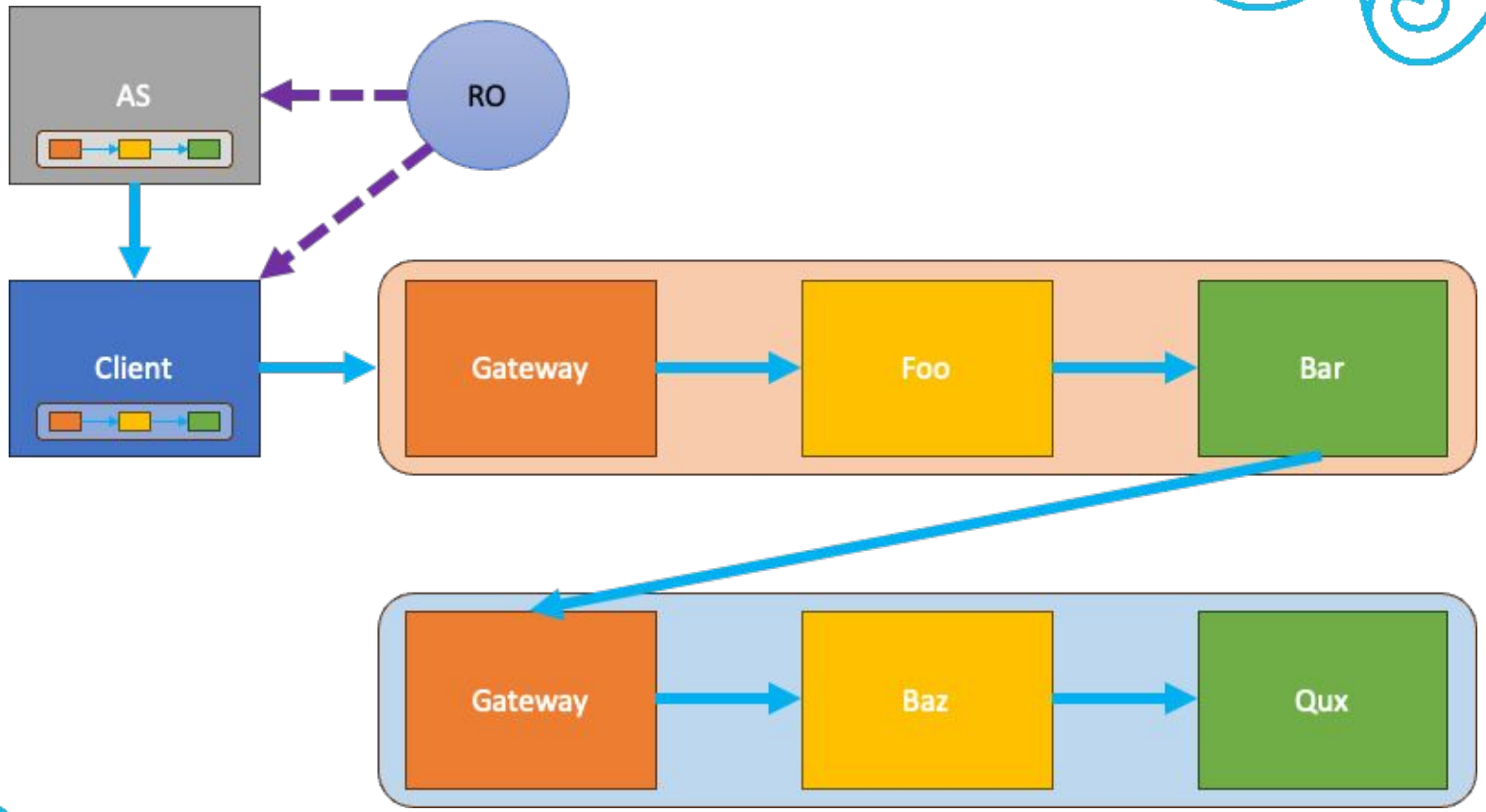
What is a *workload identity*?

a means of identifying a workload in a way that makes sense in its context



What are *multi-system environments*?

the problems don’t start and stop at cloud boundaries, we need solutions that work inside and across systems


AS
RO
Client
Gateway
Foo
Bar
Gateway
Baz
Qux

What are we doing here?

- Solving problems unique to workload environments
- Solving general problems in the unique context of workload environments
- Focus on identity and security
- Bring together lessons learned across different domains, deployments, companies, projects, and experiences
    - *People have solved many problems in this space because they had to!*

What are we not doing here?

- Inventing a grand unified protocol/system for workloads
- Static identities (SBOMs)
- Deployment systems
- Authentication of persons
- Supply chains
- Authorization engines, languages, and protocols

… but everything we do might touch these

How are we doing this?

- Immediate focus on a small set of identified key deliverables
  - Development of informational, proposed standard, BCP, and other RFC-track documents
  - Curation of use cases and other non-RFC-track artifacts
- Discussion forum for the larger workload community
  - *We can and should talk about related things that aren't in our current deliverables!*
- Liaison with other related groups in and out of IETF

Where do we put a good idea?

- Is it mostly defined somewhere else?
  - Let’s define best practices (can be opinionated)
- Could it fit better in another WG space?
  - If we’re filling gaps in other protocols, work where those protocols are
- Do we need a new standard?
  - Let’s write it!

What about other stuff?

- Our deliverables are limited, our conversation is not
  - We’re working on HTTP but need to talk about non-HTTP
  - We’re working with JOSE but need to talk about COSE and other formats
  - We’re working with token-based solutions but need to talk about alternatives
- Rechartering is an option in the future
  - As we deliver on our initial promise, we can promise more

Working Group Resources

- Mailing list: wimse@ietf.org
- GitHub: https://github.com/ietf-wg-wimse

Our First Deliverables

Securing Service-to-service Traffic

A JOSE-based WIMSE token solution to protect a chain of HTTP/REST calls, within and across trust domains. The document should support identification of microservices and cryptographic binding of the token to the caller’s identity and optionally, binding to the transaction. It should support associating context with the token, including but not limited to user identity, platform attestation, and SBOM artifacts. This deliverable includes both a token format and its usage, including binding to the caller’s identity.

Token Issuance

A document describing a method for local issuance of WIMSE tokens where the local issuer operates with limited authority. The local issuer can be the workload itself or another workload deployed nearby.

Token Exchange

Specify a protocol for exchanging an incoming token of one format for a workload-specific WIMSE token at security boundaries (possibly based on RFC 8693). Additionally, this token exchange will require specifying as proposed standard a small set of token exchange profiles (mapping of claims) between existing and new WIMSE token formats.

Token Distribution

Document and make recommendations based on operational experience to existing token distribution practices for workloads

WIMSE Architecture

The group will develop a document that defines common terminology, discusses workload attestation and identity, specifies a threat model, and defines a set of architectural components and several compositions of those components. The document will describe 2-3 scenarios and for each of them, it will identify key points needed for interoperability.

Calls for Document Adoption

Some things to keep in mind

- Deliverable : document != 1:1
- Starting documents are not final
- Starting documents are not complete

wimse@ietf.org