Secure Patterns for Internet Credentials (SPICE)

IETF 120

Note Well

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)

IETF

IETF Meeting Tips

In-person participants

- Make sure to sign into the session via Datatracker or the QR Code in this session.
- Use Meetecho (usually the “Meetecho lite”) client to:
  - join the mic queue
  - participate in shows of hands
- Keep audio and video off if not using the onsite version.

Remote participants

- Make sure your audio and video are off unless you are chairing or presenting during a session.
- Use of a headset is strongly recommended.

Agenda

Welcome - 5 min (chairs)

What is SPICE and Why Are We Here - 20 min (chairs)

SPICE and WIMSE - 5 min (Justin/Pieter)

Docs

- https://datatracker.ietf.org/doc/draft-steele-spice-profiles-bcp/ - 15 min (Mike Prorock)
- https://datatracker.ietf.org/doc/draft-prorock-spice-cose-sd-cwt/ - 15 min (Mike Prorock)

[BREAK]

- https://datatracker.ietf.org/doc/draft-steele-spice-metadata-discovery/ - 15 min (Orie Steele)
- https://datatracker.ietf.org/doc/draft-zundel-spice-glue-id/ - 15 min (Brent Zundel)

Other Business - 10min (chairs)

What is SPICE

Charter

- analyze existing and emerging IETF technologies and address any remaining gaps to facilitate their application in **digital credentials and presentations**
- develop **digital credential profiles** that support various use cases

Security & Privacy

- Implementation guidance around Privacy by Design, confidentiality, and consent
- Privacy and security considerations re:
  - confidential computing
  - remote attestation
  - trusted execution environments (TEE)
  - hardware security modules (HSM) on digital credentials
  - redaction, linkability, and selective disclosure

Coordination

- RATS (Remote ATtestation ProcedureS)
- OAuth (Web Authorization Protocol)
- JOSE (Javascript Object Signing and Encryption)
- COSE (CBOR Object Signing and Encryption)
- SCITT (Supply Chain Integrity, Transparency, and Trust)
- WIMSE (Workload Identity in Multi System Environments)

Out of Scope

- General Key discovery
- New cryptographic primitives

Working Group Resources

Mailing list: spice@ietf.org

GitHub: https://github.com/ietf-wg-spice

WIMSE

IETF120 Vancouver

Introduction for SPICE WG

What is WIMSE?

Workload

Identity in

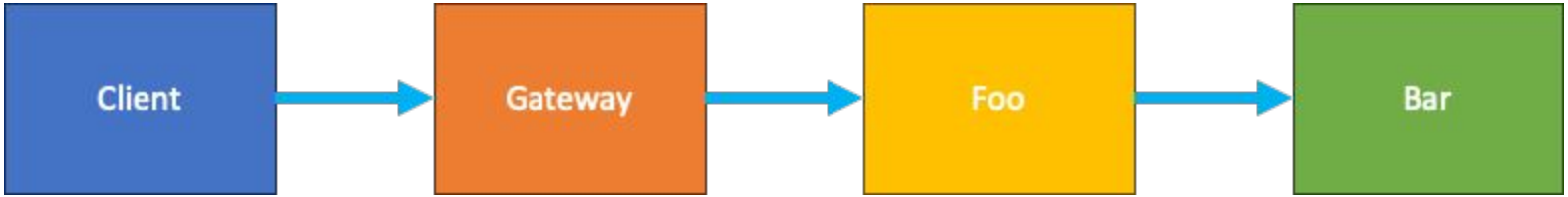
Multi-

System

Environments

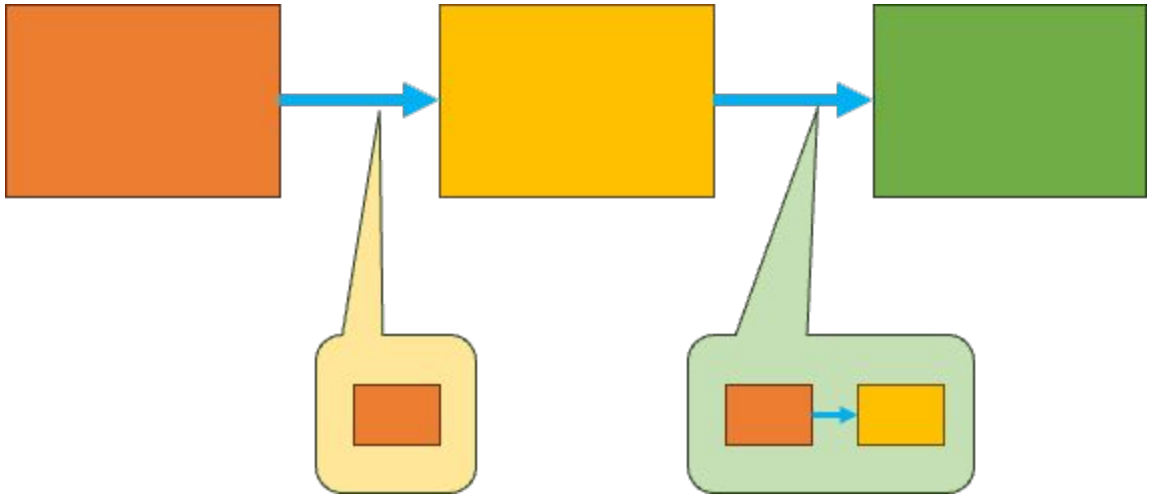
What is a *workload*?

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


Client
Gateway
Foo
Bar

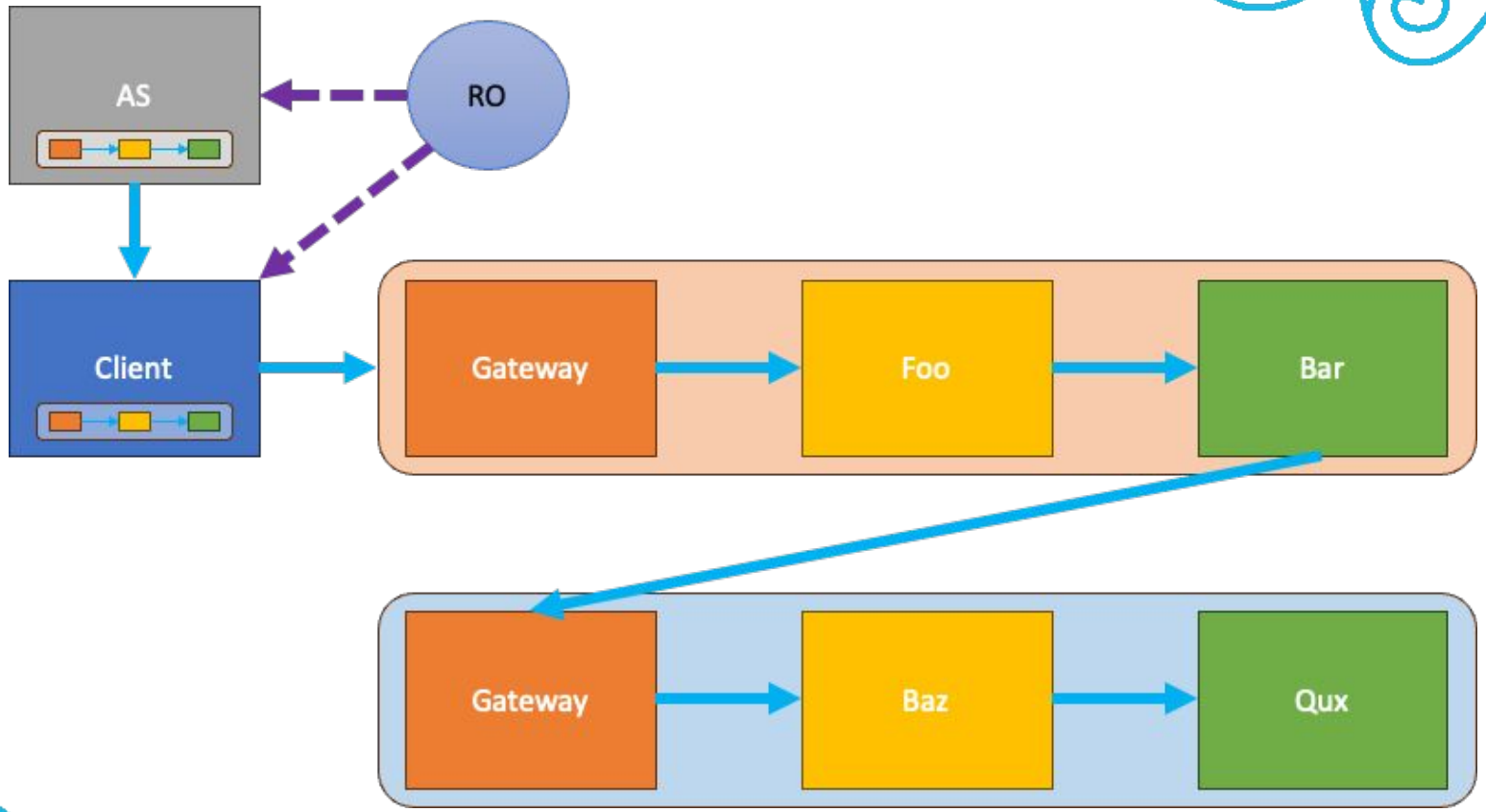
What is a *workload identity*?

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?

- 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?

- 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

wimse@ietf.org