

Trust me, Bruh.

OAuth WG
IETF123, Madrid
July 25, 2025

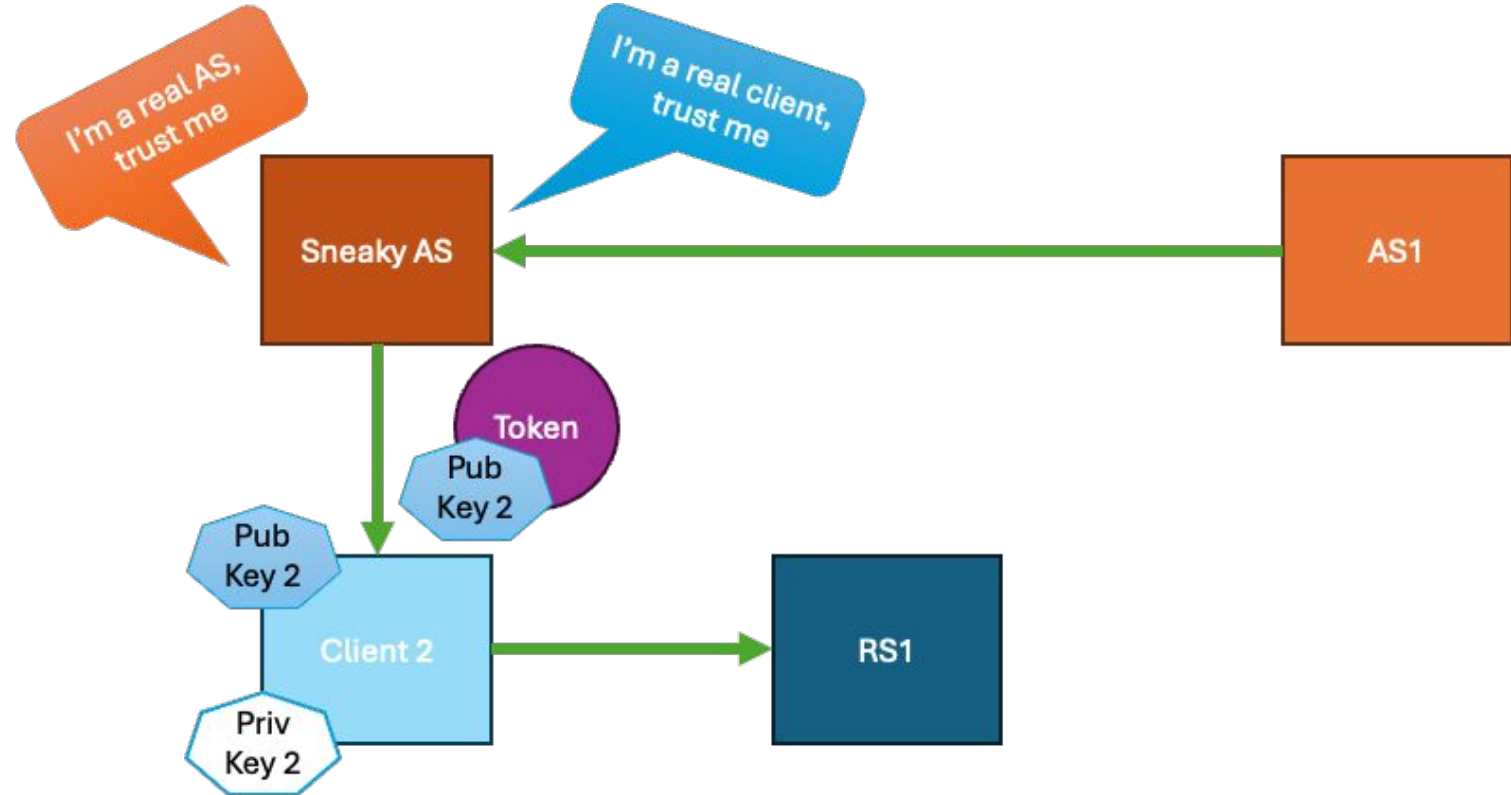
Justin Richer
Dean H. Saxe
Brian Campbell

“Deferred Token Binding”

- Bind a token to a key without presentation of proof of that key
- Defer the presentation of the bound key to later in the process

<https://www.ietf.org/archive/id/draft-richer-oauth-tmb-claim-01.html>

Why we require proof of key with the token request

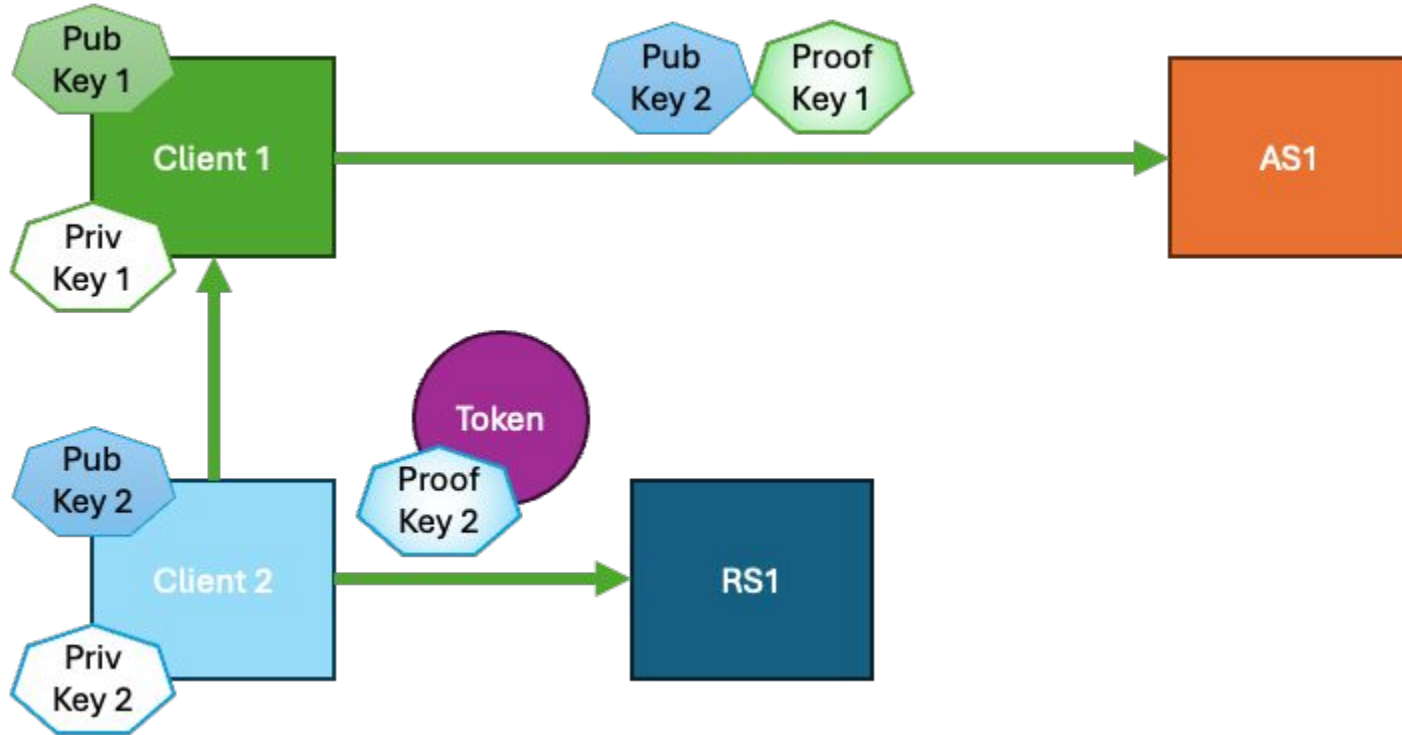


The real world isn't this simple

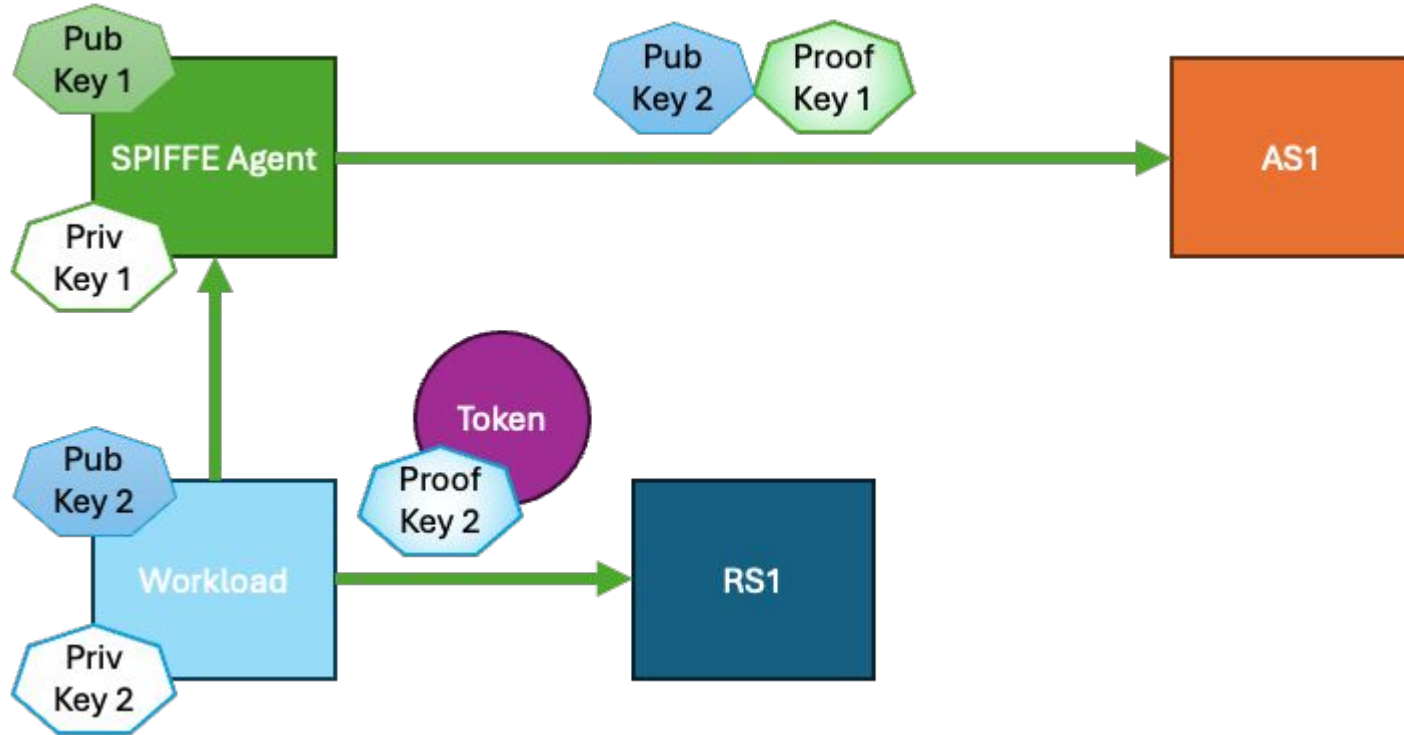
- OAuth Identity and Authorization Chaining Across Domains Appendix B.3

“In some environments, there is a need to bind the access token issued by the Authorization Server in Domain B to a private key held by the client in Domain A. This is so that the Resource Server in Domain B can verify the proof of possession of the private key of the client in Domain A when the client in Domain A presents the token to the Resource Server in Domain B.”

Key bound token on-behalf-of the key holder



Workload identities



What can we do about it?

0. Ignore it

- Write it off as “bad practice” and hope it stops

1. Informational/BCP doc

- Document existing patterns, use cases, policies, and practices
- Put up guard rails around bad practices

2. Protocol spec

- Formalize a way of asking for a token bound to some other key
- *Have some way for key presenter to create a transitive proof?*

3. Token spec

- Formalize a way of declaring a token was bound like this
- *Some flag separate from “cnf”?*