WIMSE - Credential Exchange

Individual draft submission

https://datatracker.ietf.org/doc/draft-schwenkschuster-wimse-credential-exchange/

Content

- **What situations** require a workload to obtain a different credential
- **What mechanisms exists** to obtain a (different) credential
- **Existing patterns** of exchange (and **a new one**)

Scope: Describe the meta pattern of credential exchange, not go into detail about a specific format that needs to be delivered.

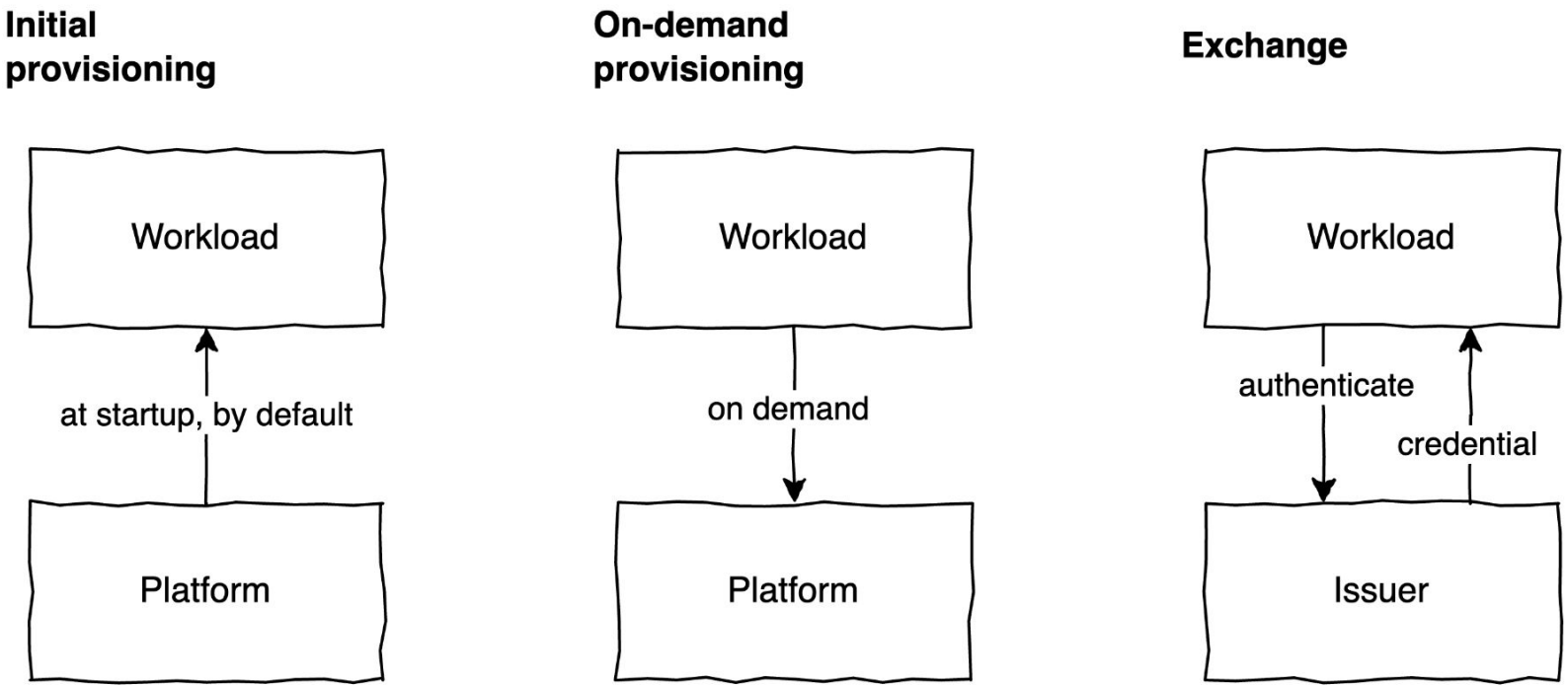
https://datatracker.ietf.org/doc/draft-schwenkschuster-wimse-credential-exchange/

“Needs”

- Change in authority
- Change in subject
- Change in scope
- Change in lifetime
- Change in format
- Missing provisioning support
- Combination of above (<- I believe this is the case most of the time)

https://datatracker.ietf.org/doc/draft-schwenkschuster-wimse-credential-exchange/

Mechanisms


Initial provisioning
Workload
at startup, by default
Platform
On-demand provisioning
Workload
on demand
Platform
Exchange
Workload
authenticate
credential
Issuer

Guidance when to use what (work in progress)

	Change in authority	Change in subject	Change in scope	Change in lifetime	Change in format	Missing provisioning support
Initial provisioning						
On-demand provisioning						
Exchange						

Existing, framework-specific exchange

- OAuth2 Token Exchange
- OAuth2 Assertion Framework

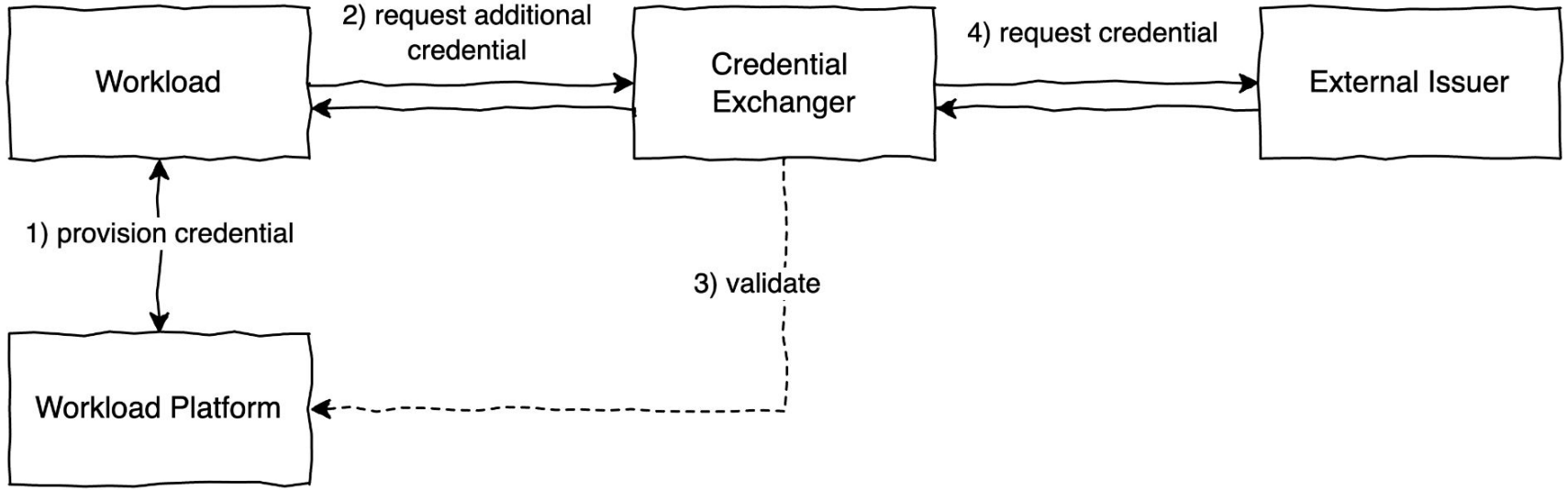
Incorporates framework- and format-specific properties: scope, subject, client authentication, etc.

Other frameworks have their own characteristics: X.509 chain building, WebPKI, SPIFFE, credential formats carrying authorization data, etc.

Learning

A silver-bullet “exchange” API doesn’t exist and would do more harm than good. Frameworks and formats vary too greatly with different security promises.

A (potential) exchange pattern - **“on behalf of”**



Current (security) considerations

- Credential exchange **cannot increase trust**
- Credential exchange **cannot replace** on-demand or initial **provisioning**
- Initial provisioning comes with **over-provisioning risk**
- Expanding credential lifetime
- Involvement of human, transactional or other contextual credentials
- Credential formats supporting offline-attenuation

Questions to the working group

- Is this something the WG wants to work on?
- Other existing, framework- or format-specific “exchange” protocols out there?
- Should we define “on-behalf-of” exchange pattern?
- Next steps?