

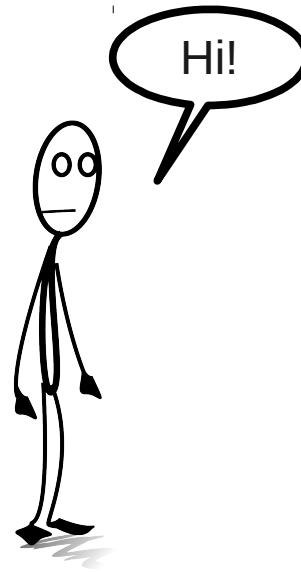


webSSO

Nathaniel McCallum
Sr. Software Engineer - Security,
Red Hat

**RED HAT®
ENTERPRISE LINUX®**

Meet AI



AI has a lot of passwords...

F!mfi1%\$fmoe

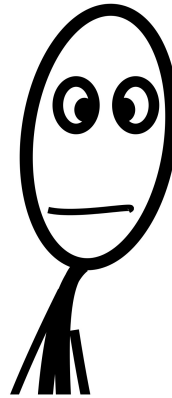
mom32

Tr0ub4dor&3

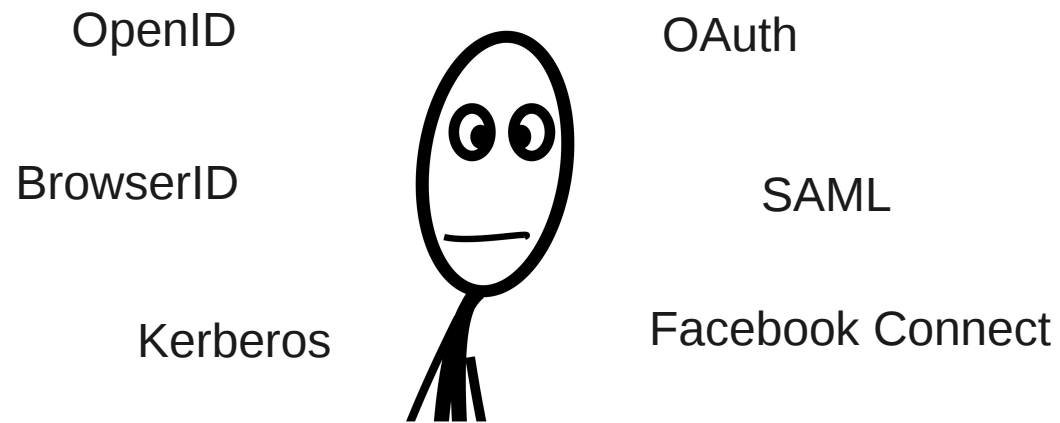
iwantaponey17

1852424

correcthorsebatterystaple

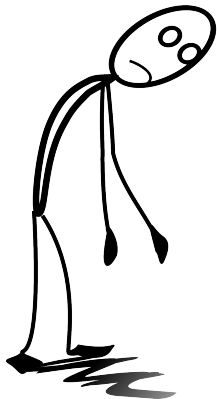


AI also has a lot of protocols...



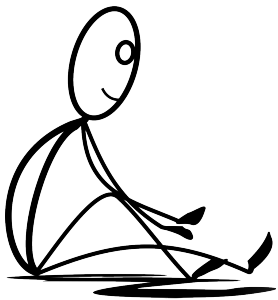
A story of protocol proliferation

1. His enterprise (Kerberos) ID is useless outside his company.
2. New Internet authentication standards don't provide SSO, are restricted to HTTP, complex to implement, have a bad security track record and lack usefulness in complex network topologies.
3. Secure sharing between data silos is an afterthought.



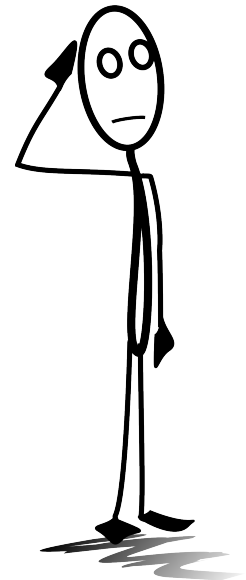
AI needs...

an easy to deploy, secure, federated SSO experience
built on scalable, web-based technologies
that transcends local, Internet and cloud infrastructure,
manages trust relationships dynamically
across complex network topology,
and handles delegation as a primary concern.

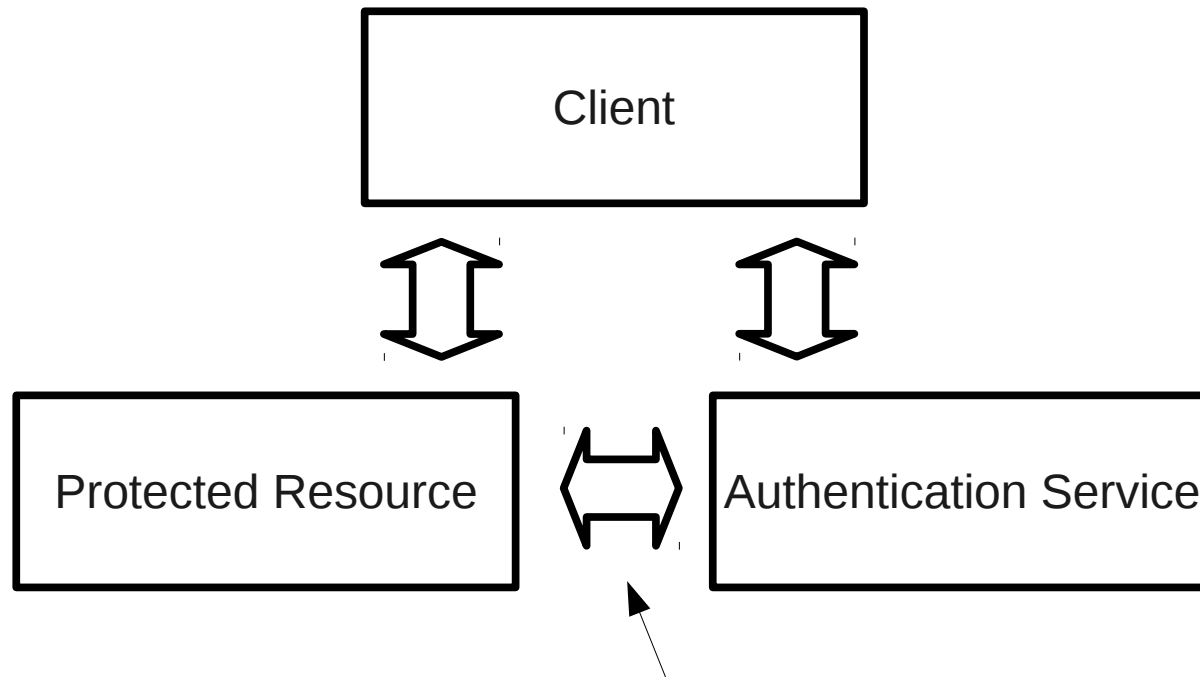
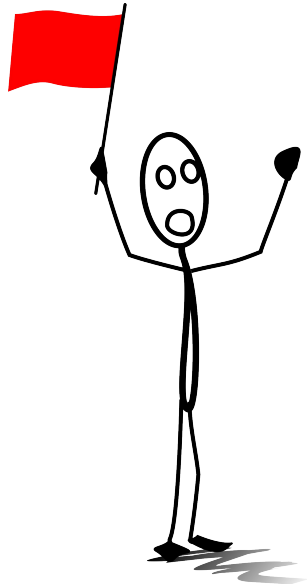


SSL/TLS Client Certificate Authentication

- ✓ easy to deploy, secure, federated SSO experience
- ✓ built on scalable, web-based technologies
- ✓ transcends local, Internet and cloud infrastructure
- ✗ manages trust relationships dynamically
- ✓ works across complex network topology
- ✗ handles delegation as a primary concern



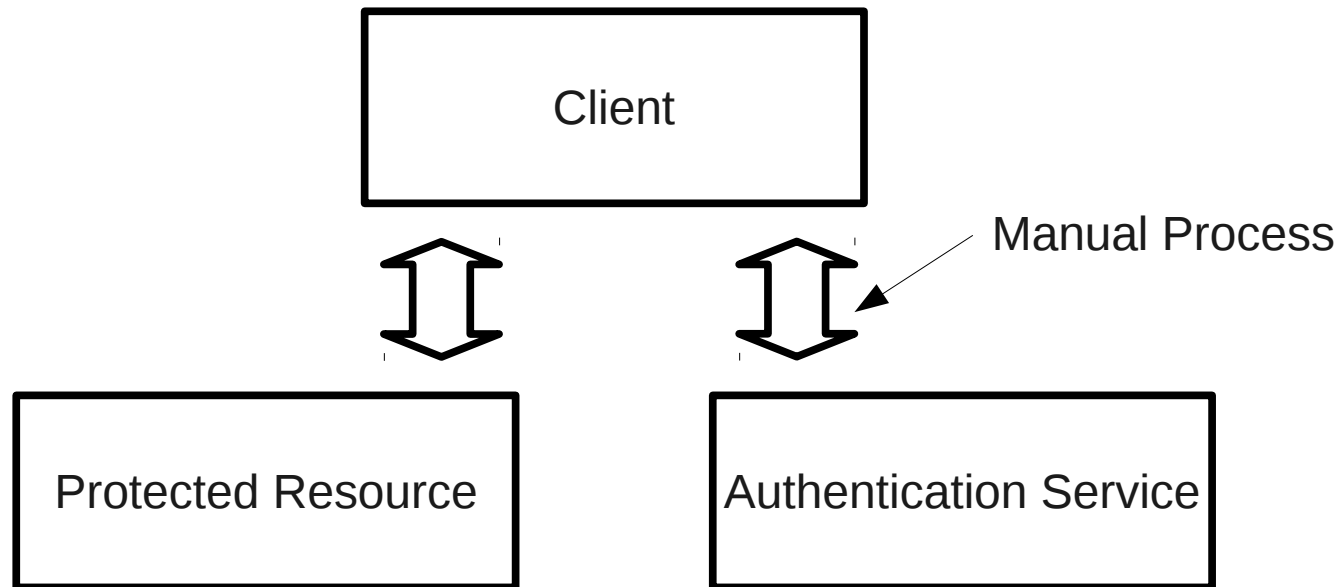
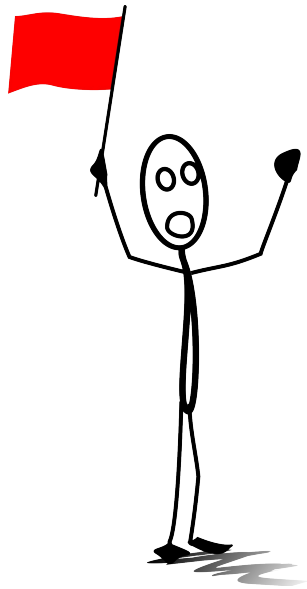
Anatomy of a Typical Authorization System



Requires AS to be publicly available



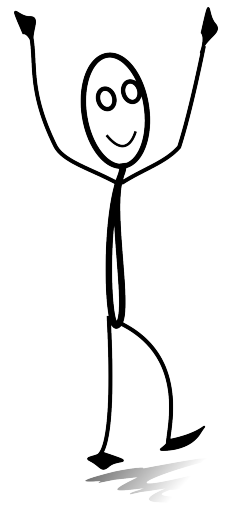
Anatomy of TLS Client Certificate Authentication



Introducing... **webSSO**

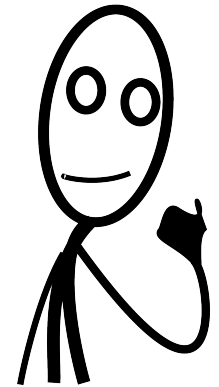
SSL/TLS Client Certificate Authentication PLUS:

- HTTP REST service for obtaining short-term certificates with full support for secure credential delegation
- Additional security validations to permit globally unique identities via established certificate authorities
- Standard client behavior for a secure (a.k.a. no phishing), polished user experience
- DNS integration

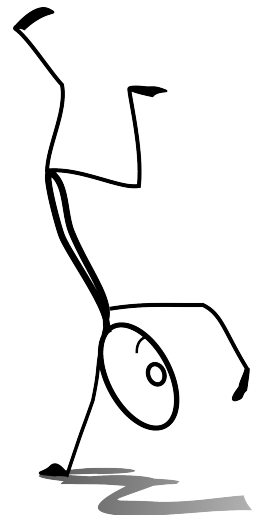
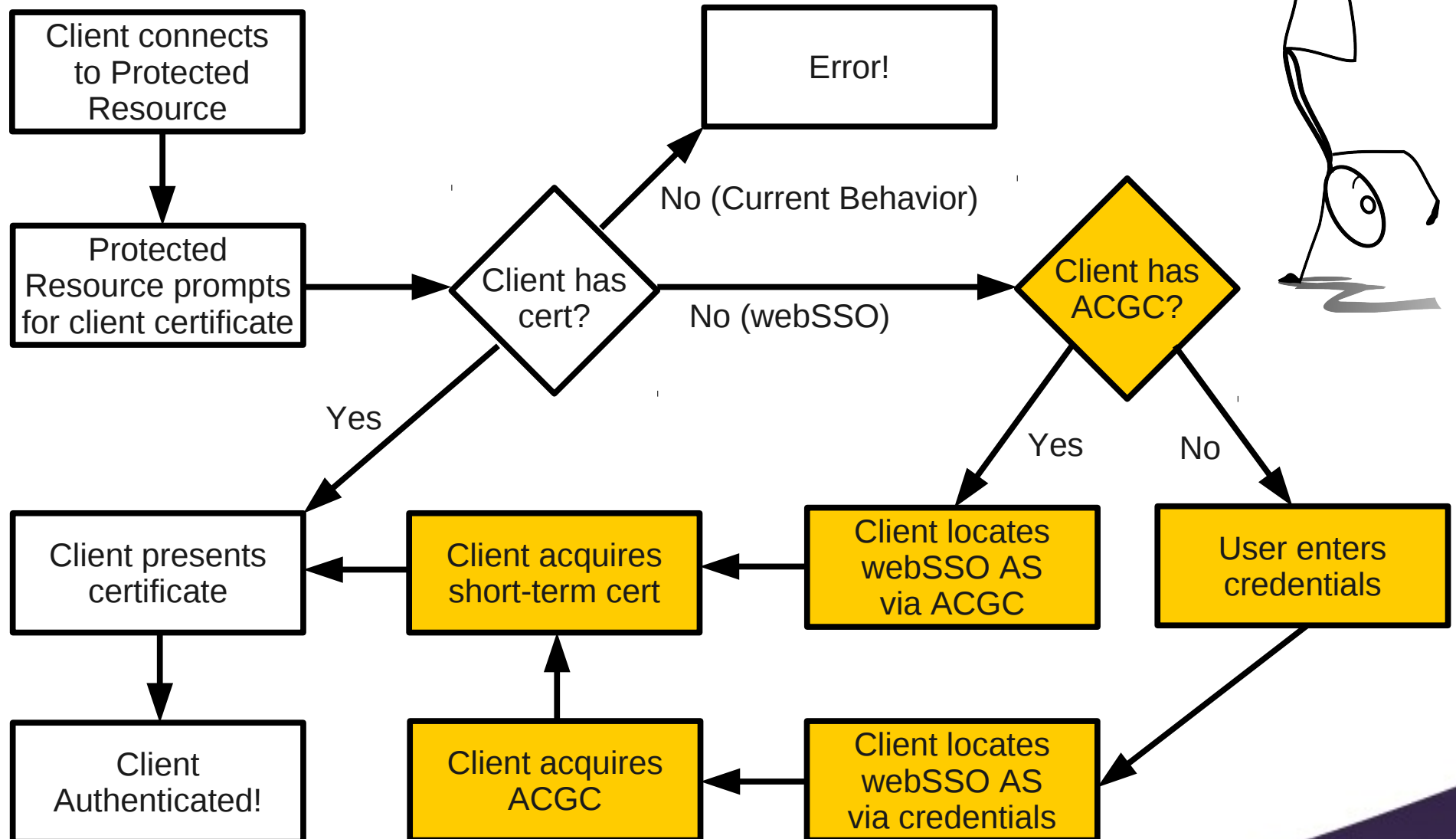


webSSO Authentication

- ✓ easy to deploy, secure, federated SSO experience
- ✓ built on scalable, web-based technologies
- ✓ transcends local, Internet and cloud infrastructure
- ✓ manages trust relationships dynamically
- ✓ works across complex network topology
- ✓ handles delegation as a primary concern

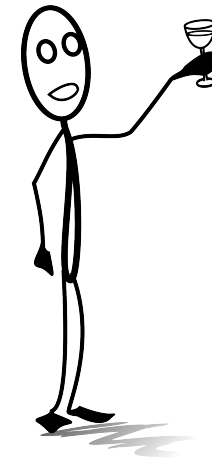


webSSO – Typical Workflow



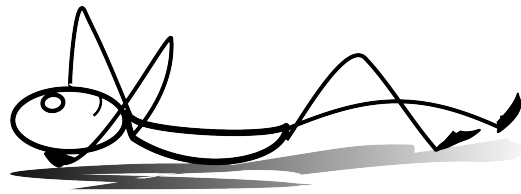
webSSO – Additional Features

- Deploys on **existing HTTP stacks**
(dynamic trust mgmt. requires additional validations)
- Verifies all parties in every transaction
- Protected resources can suggest identity providers
- Integration with existing solutions
(Kerberos, multi-factor auth, etc)



webSSO Status

- IETF Internet Draft
- User experience mock-ups
- Working webSSO AS implementation
(Apache 2.0 licensed; release imminent)



webSSO

<http://webSSO.github.com>

