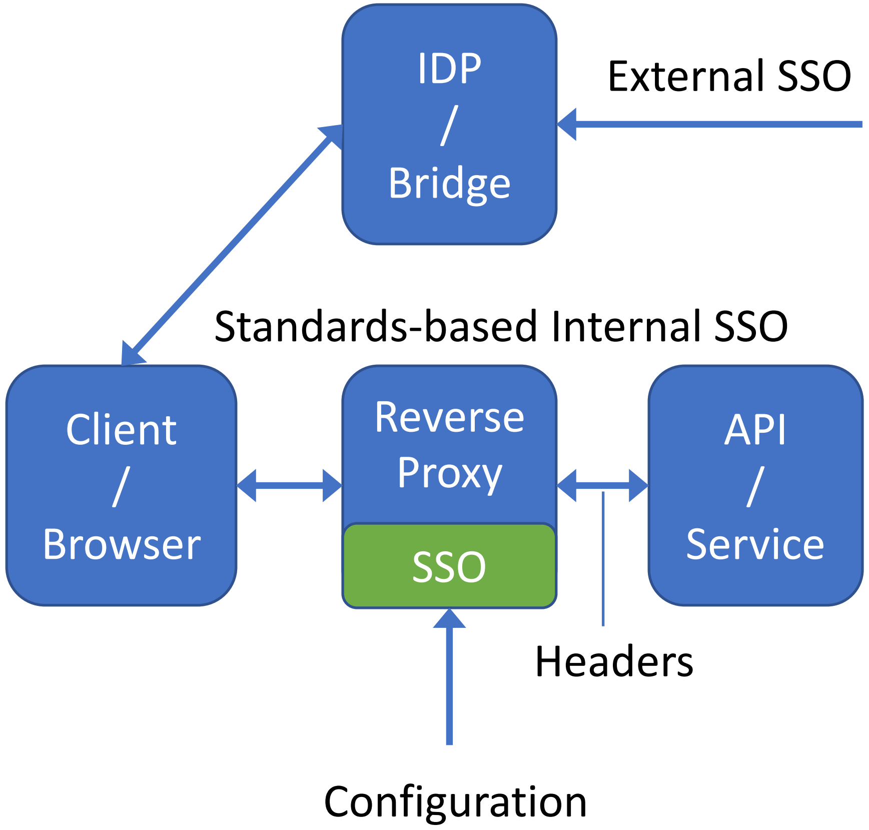
Reverse Proxy Based Single Sign On

Realizing multi-protocol Identity & Access Management architectures
with open source standards-based SSO implementations in reverse proxies.

February 12, 2019 - TIIME Workshop - Hans Zandbelt - ZmartZone IAM

Reverse Proxy Based SSO Architecture

- Externalize Auth and Authz
  - offload security from service/developer
  - delegated Management
- Well-known Architectural Pattern
  - firewall, load balancing, SSL offloading
  - can be combined with said functions
  - fit for containers / micro-services
- Configuration Managed
  - effectively realize centralized access management, obsoleting legacy WAM
- IDP is multi-protocol bridge
  - simple *internal* standardized SSO *integration* implementation/protocol replacing proprietary legacy ones



Implementation(s)

- “Integration” or “Last Mile” protocol: OpenID Connect
  - open, standardized, light-weight, widely available, modern REST/JSON nature
  - SAML 2.0: heavy-weight runtime, harder to manage/maintain/deploy, harder to implement (XML DSig), but foremost: therefore less widely available
  - because CAS or any other light-weight protocol is non-standardized

- Apache 2.x: mod_auth_openidc
  - full-featured, >100 conf primitives, in Debian/Ubuntu/Centos distro’s
- NGINX – lua-resty-openidc
  - simple, single OP, single grant type, in luarocks/opm

- In Beta
  - NGINX native module
  - Envoy Lua module
  - Generic C library (IIS, embedded etc.)