RPP – OAuth 2.0

Maarten Wullink - SIDN Labs

Pawel Kowalik - DENIC

IETF 126, Vienna, 2026

Motivation

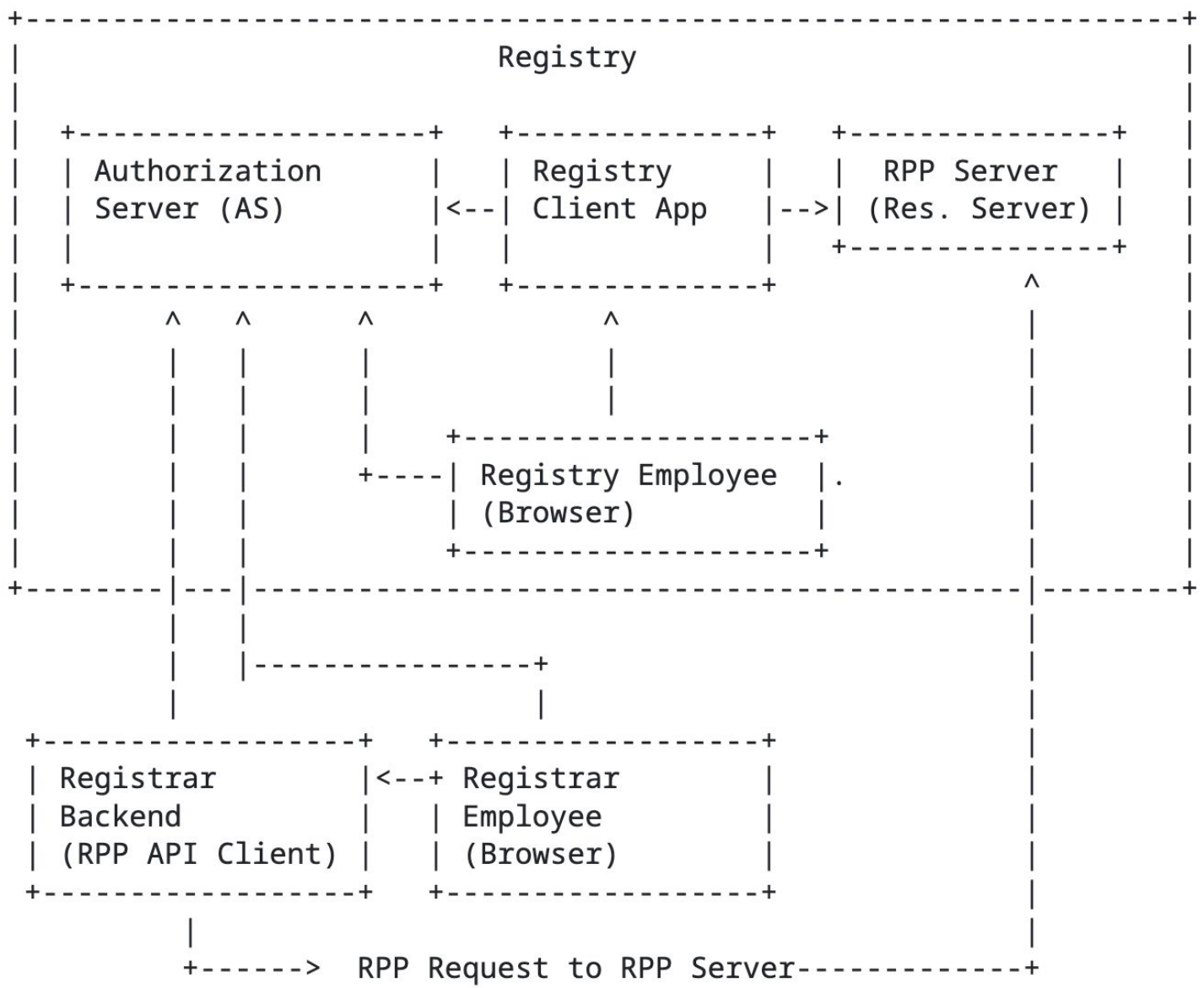
- **R9.1** RPP MUST support **state-of-the-art authentication and authorisation schemes** allowing for easy integration in modern HTTP infrastructure.
- **R9.2** RPP MUST support robust authentication and authorisation mechanisms, such as **OAuth 2.0** and OpenID Connect, to ensure that only authorised clients and users can access or modify resources.
- **R9.9** RPP MUST support a **granular authorisation matrix**, where one or more permissions are coupled to a user account. Allowing for the creation of different types of user accounts, such a readonly users only allowed to fetch data about existing objects, and power users allowed to create and modify objects.

OAuth 2.0

Both registry and registrar user authorization can be performed by the same OAuth 2.0 authorization server

- The registry can create user accounts for its support staff
- A registrar can create multiple user accounts within the registry
  - allowing registrars to self service user management would be preferred
- Fine-grained access control for both registry and registrar users
  - A user has a set of permissions (read-only, domain:create, admin etc)
- Enable registrars to implement the principle of least privilege within their own organizations.

Overview



https://datatracker.ietf.org/doc/draft-wullink-rpp-oauth2-delegation/

Authentication Flows

OAuth 2.0 supports

- **Interactive:** For real users interacting with the system via browser
- **Machine-2-machine**: For automated registrar systems

Scopes

OAuth 2.0 scopes are used for granting authorization and enforcing access control when accessing RPP resources.

RPP uses standard scopes such as “sub” and “iss” (RFC9068) but also introduces set on new scopes

- Scopes are derived systematically from the data object
- The scope identifier MUST use the format <object>:<access-level>
- The user request 1 or more scopes during login

Scopes

Scope example for domain object

Scope	Data Object	Operations Granted
domain:create	Domain Name	Create
domain:read	Domain Name	Read
domain:update	Domain Name	Update
domain:renew	Domain Name	Renew

Claims

New RPP-specific claims are defined to enable fine-grained authorization decisions

The “sub” scope together with following claims identify a user:

- rpp_registrar_id (Required)
- rpp_reseller_id (Optional)

Future Work

- Update draft based on feedback
- OAuth 2.0 support is NOT going to be included in RPP core
- Low(er) priority when Secure Transfer and Secure Delegation Management do not require OAuth 2.0 support.

Thank You

www.sidnlabs.nl | stats.sidnlabs.nl