



IETF 125

RPP Architecture Update

Pawel Kowalik (DENIC)
Maarten Wullink (SIDN)

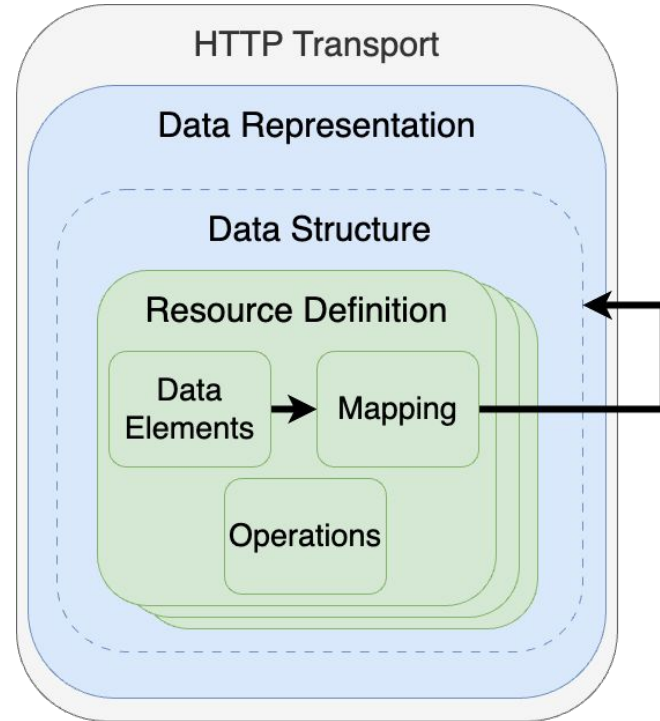


Recap on the document

- WG adopted document
- Target status: Informational (parked)
- [draft-ietf-rpp-architecture-01](#)

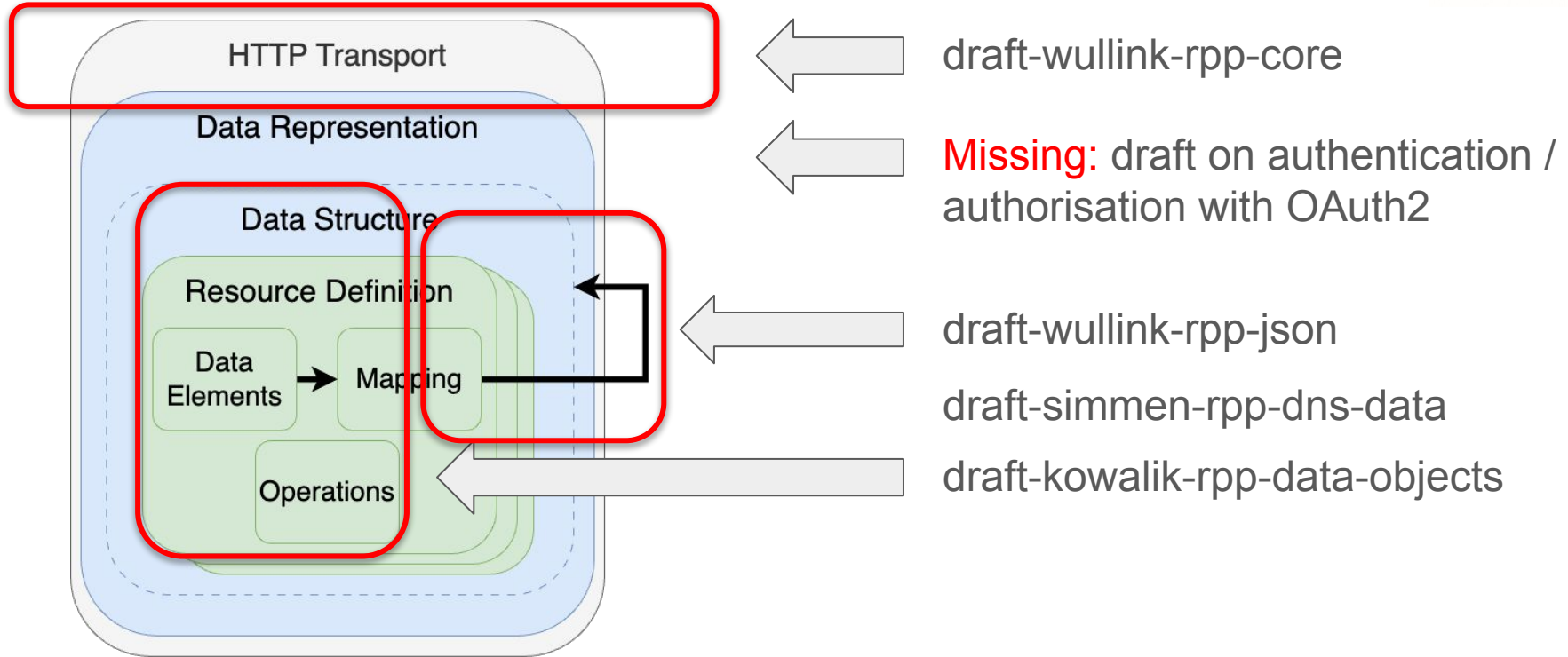
Layered architecture:

- Following Resource Oriented Architecture principles
- Use as much from HTTP and related standards as possible





Mapping on documents





-01 version published

- Changes generally to cover missing items from draft-ietf-rpp-requirements-03
 - Extension Mechanisms - transient request parameters and responses, HTTP headers, security
 - Service Discovery & Profiles - compatibility profiles, data privacy, maintenance notices
 - Security & Authentication - TLS requirements, credential management and lifecycle (revocation), optional message signing, object level authorisation
 - Collections, Bulk Operations & Filtering - collection representation, optionality on bulk functions, listing, filtering
 - HTTP Layer - canonical addressing, usage of status codes
 - Resource Definition & Data Model - relationships, required and optional data elements, server-managed resources,
 - Poll messages
 - Message validation handling from lenient to strict



Discovery document freshness

- server configuration is considered static between its reconfigurations
- versioning mechanism for the service discovery document
- How clients would be aware of new version of discovery document?
 - Option 1: mutual signalling (i.e. dedicated header or media type parameters)
 - Benefit: servers would know what version clients use, can warn outdated clients
 - Cost: additional processing by the server for each request
 - Option 2: polling with http cache mechanisms
 - Benefit: (almost) no overhead for servers
 - Cost: no knowledge at the server about discovery document freshness by the client



Login Security Extension RFC8807

- policies related to authentication or authorisation -> delegated to authentication schema
- metadata about the client (user agent) - app, os, tech information.
 - Easy solution: User-Agent header. Is all data from RFC8807 useful with each request? Any WG feedback what is useful?
- loginSec:event
 - if authentication is delegated, then the events won't happen on protocol level, but interaction between client and auth server
 - for basic auth it might be not practicable to deliver such events for each request. Basic auth shall be considered "legacy" back-compatibility with EPP, not target solution
 - RPP has a generic warning/info mechanism - is it enough for basic auth case?



Simplified and quicker object transfer process

- R9.3 Support for a simplified and quicker object transfer process MAY be included, where approval from the losing registrar is to be obtained interactively by the registrant during the transfer process.
- So far we don't have good idea for this - delegated end user (domain owner) authentication and transfer authorisation is in core of the problem
 - See discussions on [AuthCodeSEC EPP extension](#) in REGEXT
- Proposal: park it (it's MAY), unless there is someone willing to take a lead on this part



Next steps

- ~~review again against final requirements~~ ✓
- full WG reviews are needed !!
- Ready for WG Last Call?
- early reviews from other WGs / directorates? HttpDir?



Thank you

- ▷ Email: pawel.kowalik@denic.de
- ▷ LinkedIn: <https://www.linkedin.com/in/pawelk/>
- ▷ Mastodon: <https://mastodon.social/@paulok>
- ▷ Bluesky: <https://bsky.app/profile/pawel.paulonet.eu>