

Background on EPP

Gavin Brown, RPP BOF, IETF 121, Dublin, November 2024

Agenda

- A description of the Extensible Provisioning Protocol (EPP) for the uninitiated.
- The role of EPP in the generic TLD namespace.
- How a new provisioning protocol might be deployed in the gTLD namespace.

What is EPP?

EPP is “an application-layer client-server protocol for the provisioning and management of objects stored in a shared central repository.”

EPP is:

1. A data model;
2. A command repertoire;
3. A transport protocol.

These components are loosely coupled, and can be swapped out without affecting the other components.

See: STD 69

The EPP data model

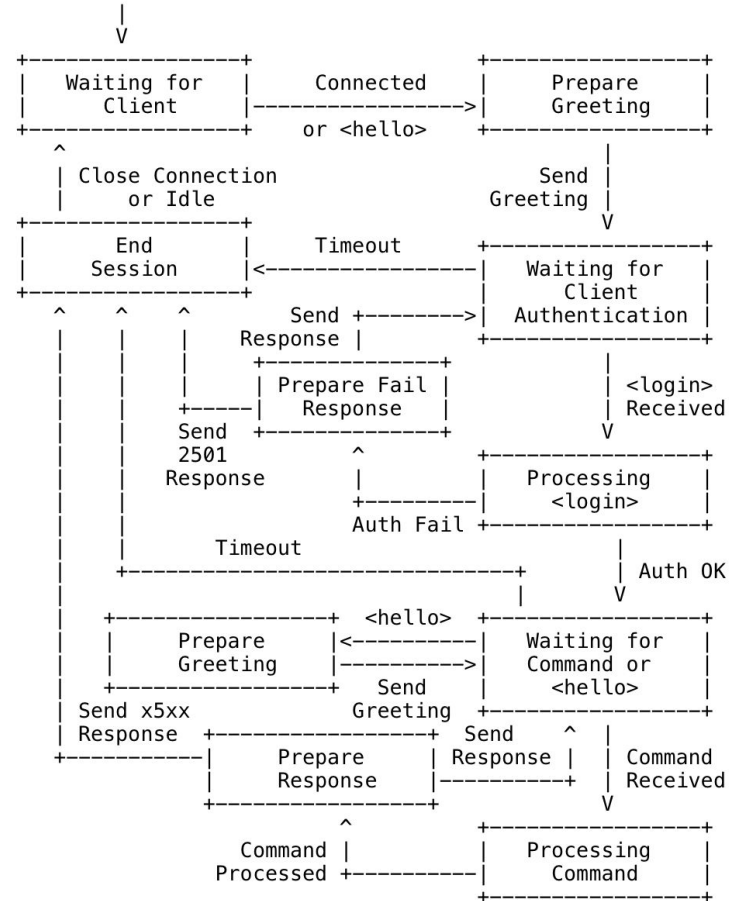
- Is expressed in XML;
- Uses *XML namespaces* to uniquely identify object types;
- Uses *XML schemas* to describe (and allow validation of) objects;
- Uses common elements across object types;
- Implements a “sponsorship” model;
- Is extensible by using new namespaces.

The EPP command repertoire

- Provides CRUD verbs (<create>, <info> <update>, <delete>) plus <check>, <renew>, <transfer>.
- <poll> to access the message queue.
- Is extensible, again by using new XML namespaces.

EPP transport protocols

- Guidelines for transports are set out in RFC 5730, Section 2.1.
- TLS transport specified in RFC 5734.
- Specifications exist for transports based on HTTP and QUIC.
- Deployments of EPP over HTTP have existed for many years.



The role of EPP in the gTLD namespace

The SRS Model

- All gTLDs* operate under a “Shared Registry System” model: one registry (the “wholesaler”), many registrars (the “retailers”).
- Both registries and registrars have contracts with ICANN which govern certain aspects of how they interact with each other.
- The Registry Agreement (RA) governs what “services” a registry MUST, MAY and MUST NOT offer.

** This restriction is somewhat relaxed for “brand” TLDs.*

The MUSTs

- “Critical functions” are things that a registry MUST do (and meet an SLA for):
 1. DNS;
 2. DNSSEC;
 3. Data Escrow;
 4. RDDS (RDAP & WHOIS);
 5. EPP.

The MAYs

- Registry operators MAY offer additional services, but must comply with the Registry Services Evaluation Policy (RSEP).
- This policy defines products or services that require ICANN review prior to being offered.
- ICANN reviews the proposed service to see if it poses any security or stability risks, or competition issues.
- ICANN then provides authorisation to the registry operator to offer the proposed service.

New provisioning protocols

- A registry operator may offer a new provisioning protocol to its registrars, provided:
 - They continue to offer EPP in accordance with the Registry Agreement;
 - They submit an RSEP request, and the review raises no new security, stability or competition concerns.
- A proposed change to the base RA for TLDs established in the Next Round would allow ICANN to proactively review new technologies and services and publish a list of “elective” services on its website.

Transitioning of critical functions to new protocols

- Until EPP is removed from the RA as a critical function, any new provisioning protocol would have to coexist alongside it.
- Such a change would require consensus from across the community.
- This has happened to another protocol:
 - RDAP became mandatory in August 2019;
 - WHOIS will become optional as of January 2025.

ICANN and IETF working groups

- ICANN policies have no special standing in relation to IETF working groups.
- The work of the IETF serves the entire world, not just generic TLDs.
- The fact that a gTLD registry operator has to comply additional requirements before offering a new protocol should not decide whether or not the work to specify that protocol should be done (in the IETF or anywhere else).

Thanks