The Paypal REST API Standards

Eric Jacolin

WOSSAT meetup - 2019-02-19

What and why?

- Paypal have produced a superb REST API standards and shared it (Sept 2017) – Adopt it as your organisation's standard!
- Comprehensive, intuitive, convenient
- The right amount of detail
- Easy to share between team members and refer to, easy to embed in your organisation's culture
- Covers almost all the patterns you will ever need
- You can extend it as you please

API Design Guidelines

- https://github.com/paypal/api-standards/blob/master/api-style-guide.md
- Service design principles (loose coupling, encapsulation, stability, reusability, etc.)
- Proper use of HTTP verbs, status codes, headers
- A standard for HATEOAS links
- Naming conventions for URI components (resources, subresources, namespaces)
- Immutable identifiers
- Error handling (error.json, error catalogue)
- API versioning (uses semantic versioning)
- Different types of APIs (capability, experience, process)

API Design Patterns and Use Cases

- https://github.com/paypal/api-standards/blob/master/patterns.md
- Search type resources on collections (time selection, sorting, pagination, query parameters, response properties: total items, total pages, links)
- Read/ delete/ update single resource
- PATCH partial update, concurrency protection with Etag or JSON pointer expression (use with care)
- Projected response (list of fields required)
- Asynchronous operations (return a final rel=self URI or a temporary request queue URI)
- Controller pattern:
  - POST to non-resources: simulation, calculations
  - Complex operations: update several resources
- File upload (multipart/form-data)
- Bulk operations

Typical extensions

- Error handling on complex operations (when a leg of the orchestration fails)
- Security context: usually provided in a HTTP Authorization header (basic auth, API key, JWT access token, ...)
- Unique request id for tracking purposes (in custom HTTP header)
- Sensitive resource ids: for ex. credit card numbers => can't use GET to read resources
- Version nb in a HTTP Accept header instead of in the URL