Extending HTTP for fun and non-profit

How the API Italian Interoperability Framework is contributing to global standards

Europython 2020

Roberto Polli
API Ecosystem
AGENDA

How writing the Italian API Guidelines led us to contribute to the HTTP community

→ Writing API guidelines
→ Identify standards and communities
→ Writing an Internet-Draft
→ The RateLimit headers Draft
THE CHALLENGE

Standardizing all public sector APIs

Guidelines can uniform APIs produced by thousands of service providers

60M People
+12k Public Agencies
+8k Cities
20 Regions
(∞ cultural heritage)
API GUIDELINES RISKS

Technical guidelines

Risks

Technical specifications in government risk to mimic a bureaucratic environment

- **over-complexity**: bureaucratic non-digital processes are mapped to convoluted APIs without a proper redesign

- **time-constrained engineering**: a restricted groups of people addressing the above use-cases within a short deadline

- **closed development**: the IT community is rarely involved. Development happens in a close environment. Sometimes even the specifications are closed

- **redundancy**: when built on variation of existing standards without keeping in touch with the original communities
GOALS AND KEY FEATURES

Identify Guideline goals and key features

To write a guideline you have to prioritize goals and features: this eases the stakeholder identification and the feature landscaping.

➔ Consistent Design & Schema standardization: introduce design rules and standard schemas to uniform APIs between different agencies

➔ Reliability & Security: enforce a service management model addressing cascading failures and security frameworks lowering legal risks for providers

And always... engage and create Communities: government, developers, implementers and standards
GOALS AND KEY FEATURES

Schema
Design
Reliability
Security

IDENTIFY GOALS - pick your own!
<table>
<thead>
<tr>
<th>GOALS AND KEY FEATURES</th>
<th>National</th>
<th>EU</th>
<th>IETF, W3C, ...</th>
<th>Communities</th>
<th>Vendors</th>
</tr>
</thead>
<tbody>
<tr>
<td>Schema</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Design</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Reliability</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Security</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
## Adopting and Proposing Standards: An Excerpt

<table>
<thead>
<tr>
<th>Schema</th>
<th>Design</th>
<th>Reliability</th>
<th>Security</th>
</tr>
</thead>
<tbody>
<tr>
<td>RFC7807, RFC3339, ISO4217, BCP47, RFC8259, ..</td>
<td>HTTP (RFC723x), OpenAPI</td>
<td>HTTP, TBD:service-management</td>
<td>JWx, Digest, I-D.signed-exchanges, TBD:non-repudiation</td>
</tr>
<tr>
<td>OpenAPI, IETF, Jsonschema, HL7</td>
<td>OpenAPI, HTTP</td>
<td>IETF, ISO</td>
<td>IETF, W3C, HTTP, Banking APIs</td>
</tr>
</tbody>
</table>

Communities

**Fill the cells with specs, products, communities,**
Case study: a non-repudiation framework based on HTTP.

Study existing solutions and relevant technologies, including experimental proposals.

Identify the various building blocks, which parts are not covered by standards, or have divergent implementations.

In our case, we focused on the simplest building block: the integrity of the payload body via Digest HTTP header.

Find missing use-cases and propose solutions

Research and analyse actual solutions, even if not standard, and include experimental work or research papers.
CASE STUDY

Participating to global standards

Engaging the HTTP community while facing data integrity in REST, gave unexpected outcomes.

Our experience with the Digest HTTP Header:

- **draft a standard solution** fixing existing loopholes and adding examples
- **engage with communities, suppliers and vendors**, look for co-editors, get feedback and awareness from implementers
- **get consensus inside IETF**, resulting in the adoption of the Digest Internet-Draft
- **contribute**: continue working until the Internet-Draft becomes a standard RFC

We joined the community as volunteers for an "housekeeping work".
Provides content integrity in various APIs included banking ones.

Widely used in conjunction with signatures.

Adapted to latest HTTP specifications.

Better security considerations, covering signature usage.

Clarify ambiguities found in its usage adding examples.

Abstract
This document defines the Digest and Want-Digest header fields for HTTP, thus allowing client and server to negotiate an integrity checksum of the exchanged resource representation data.

This document obsoletes RFC 3230. It replaces the term "instance" with "representation", which makes it consistent with the HTTP Semantic and Context defined in RFC 7231.

Note to Readers
RFC EDITOR: please remove this section before publication.

Discussion of this draft takes place on the HTTP working group mailing list (ietf-http-wg@w3.org), which is archived at https://lists.w3.org/Archives/Public/ietf-http-wg/ [1].

The source code and issues list for this draft can be found at https://github.com/httpwg/http-extensions [2].

Internet-Draft is submitted in full conformance with the provisions of BCP 78 and BCP 79.

Internet-Drafts are working documents of the Internet Engineering Task Force (IETF). Note that other groups may also distribute working documents as Internet-Drafts. The list of current Internet-Drafts is at https://datatracker.ietf.org/drafts/current/.
CASE STUDY

Iterate!

Working on Digest we made friendship with the HTTP community and learnt many interesting HTTP features

Our experience with the Digest HTTP Header:

➔ got social with other HTTP experts
➔ knowledge of IETF processes
➔ got involved in other HTTP specs
➔ discovered HTTP/3 and other features

Iterate on another missing use-case!
Every API gateway implements its own ratelimit headers.

Thus many clients ignore them.

Standardize three headers

RateLimit-Limit
RateLimit-Remaining
RateLimit-Reset

Working with suppliers and cloud providers to implement them.
Digest Headers
We maintain the new I-D for the Digest header. Contributions are welcome on the IETF http-extension github repository.

Rate-Limit Headers
We proposed a new I-D allowing servers to publish current request quotas and clients to shape their request policy and avoid being throttled out. https://tinyurl.com/draft-ratelimit-html

OpenAPI: Mutual TLS and Summary
OpenAPI is WSDL for REST. We supported the inclusion of mutualTLS and the "summary" field into the new 3.1 version.

HTTP Signatures
We participate to the discussion on HTTP Signatures which is used by many banking APIs sign transactions.

API metadata in OpenAPI
Exposing API maturity and lifecycle informations into OpenAPI #1973. Considering well-known URIs for exposing service documentation and description.

Suppliers & Community
Supporting our Guidelines in various opensource software and between suppliers and vendors.

- WSO2 pull/7059
- Apicast issues/953, pull/929
- Kong issues/233/
- SaaS providers: reporting-throttling-information, openapi3
Contacts

Roberto Polli
• Email: roberto@teamdigitale.governo.it
• GitHub: ioggstream

www: https://innovazione.governo.it
twitter: @InnovazioneGov
An Interoperability Framework for Public Services should be:

➔ Oriented on data (resources) rather than processes
➔ independent from technological architectures (eg. gateways, ..)
➔ based on industry and the facto standards used on the internet by the IT industry

Public sector should:

➔ participate to the creation of industry standards to ensure that gov’t use cases are represented in the appropriate fora
➔ coordinate when doing so

Main takings on interoperability while writing the framework and confronting with agencies and countries.
Technical interoperability affects user experience.
### Adopting and proposing standards: an excerpt

<table>
<thead>
<tr>
<th>Schema</th>
<th>Design</th>
<th>Reliability</th>
<th>Security</th>
</tr>
</thead>
<tbody>
<tr>
<td>National ontologies and shared repos</td>
<td>Guidelines, REST</td>
<td>Guidelines provided a basis for IETF contributions</td>
<td>Guidelines provided a basis for IETF contributions</td>
</tr>
<tr>
<td>RFC7807, RFC3339, ISO4217, BCP47, ..</td>
<td>HTTP, OpenAPI 3</td>
<td>RateLimit Headers, HTTP</td>
<td>JWT, Digest, HTTP Signatures</td>
</tr>
<tr>
<td>OpenAPI, IETF</td>
<td>OpenAPI, Providers, Vendors</td>
<td>IETF, Vendors</td>
<td>IETF, W3C</td>
</tr>
</tbody>
</table>

We joined the underlined spec/workgroups.
Piattaforma abilitatrice all’accesso a servizi pubblici e privati, fisici e digitali

Semplificazione nelle procedure di identificazione in area Schengen e nei paesi con accordi bilaterali ai gate