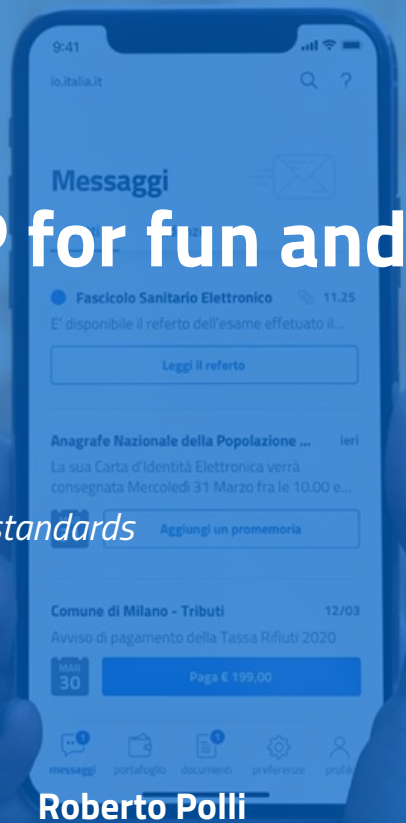
Extending HTTP for fun and non-profit

How the API Italian Interoperability Framework is contributing to global standards

Europython 2020



MINISTRO PER L'INNOVAZIONE TECNOLOGICA E LA DIGITALIZZAZIONE

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)

MINISTRO
PER L'INNOVAZIONE
TECNOLOGICA
E LA DIGITALIZZAZIONE

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

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

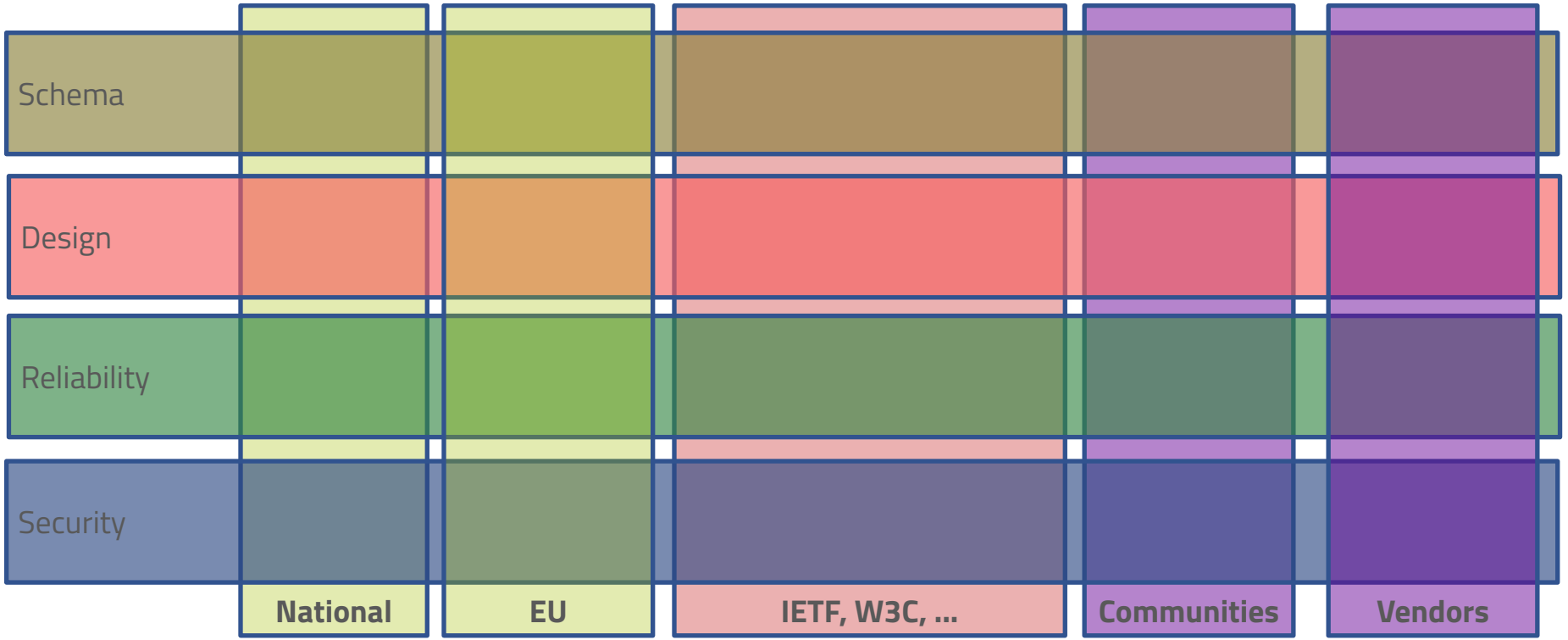
And always... **engage and create Communities**: government, developers, implementers and standards

GOALS AND KEY FEATURES

MINISTRO
PER L'INNOVAZIONE
TECNOLOGICA
E LA DIGITALIZZAZIONE

IDENTIFY GOALS - pick your own!

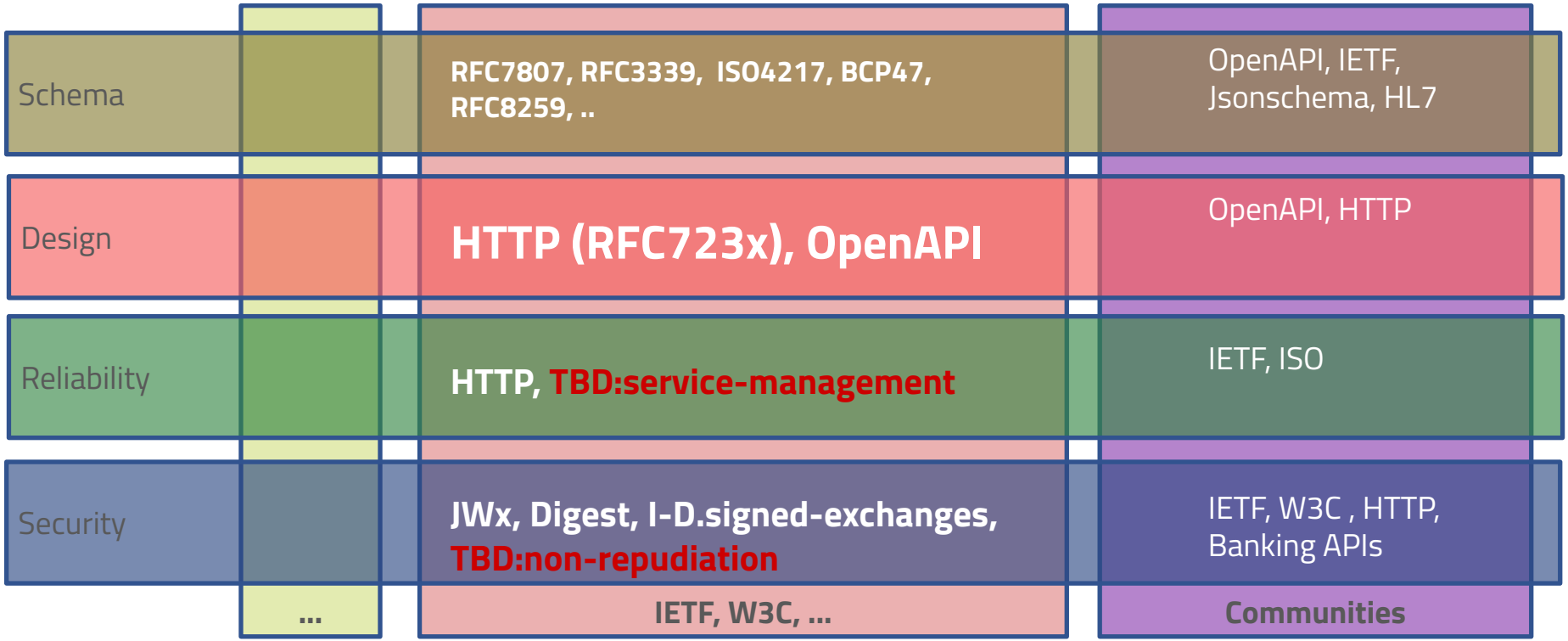
GOALS AND KEY FEATURES



MINISTRO
PER L'INNOVAZIONE
TECNOLOGICA
E LA DIGITALIZZAZIONE

IDENTIFY COMMUNITIES - pick your own

ADOPTING AND PROPOSING STANDARDS: AN EXCERPT



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: 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.

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".

Digest Header

Users

Provides content integrity in various APIs included banking ones.

Widely used in conjunction with signatures.

Ideas

Adapted to latest HTTP specifications.

Better security considerations, covering signature usage.

Clarify ambiguities found in its usage adding examples.

```
HTTP                                                          R. Polli
Internet-Draft                          Team Digitale, Italian Government
Intended status: Standards Track                              L. Pardue
Expires: January 5, 2020                                      Cloudflare
                                                          July 04, 2019


                        Resource Digests for HTTP
                    draft-ietf-httpbis-digest-headers-00

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.

te to Readers

_RFC EDITOR: please remove this section before publication_

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

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

 of This Memo

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

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

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!

RateLimit Headers

Users

Every API gateway implements its own ratelimit headers.

Thus many clients ignore them.

Ideas

Standardize three headers

`RateLimit-Limit`
`RateLimit-Remaining`
`RateLimit-Reset`

Working with suppliers and cloud providers to implement them.

TEAM PER LA TRASFORMAZIONE DIGITALE

```
Network Working Group                                          R. Polli
Internet-Draft                          Team Digitale, Italian Government
Intended status: Standards Track                            A. Martinez
Expires: April 23, 2020                                        Red Hat
                                                        October 21, 2019

                RateLimit Header Fields for HTTP
                draft-polli-ratelimit-headers-01

Abstract

   This document defines the RateLimit-Limit, RateLimit-Remaining,
   RateLimit-Reset header fields for HTTP, thus allowing servers to
   publish current request quotas and clients to shape their request
   policy and avoid being throttled out.

1.  Introduction

   The widespreading of HTTP as a distributed computation protocol
   requires an explicit way of communicating service status and usage
   quotas.

   This was partially addressed with the "Retry-After" header field
   defined in [RFC7231] to be returned in "429 Too Many Requests" or
   "503 Service Unavailable" responses.

   Still, there is not a standard way to communicate service quotas so
   that the client can throttle its requests and prevent 4xx or 5xx
   responses.
```

OTHER SPECIFICATIONS AND COMMUNITIES WE ARE INVOLVED WITH

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

·MID

MINISTRO
PER L'INNOVAZIONE
TECNOLOGICA
E LA DIGITALIZZAZIONE

·MID

Contacts

Roberto Polli

- Email: roberto@teamdigitale.governo.it
- GitHub: ioggstream

www: https://innovazione.governo.it
twitter: @InnovazioneGov

Images from unsplash

Main takings on interoperability

while writing the framework and confronting with agencies and countries.

TEAM PER LA TRASFORMAZIONE DIGITALE

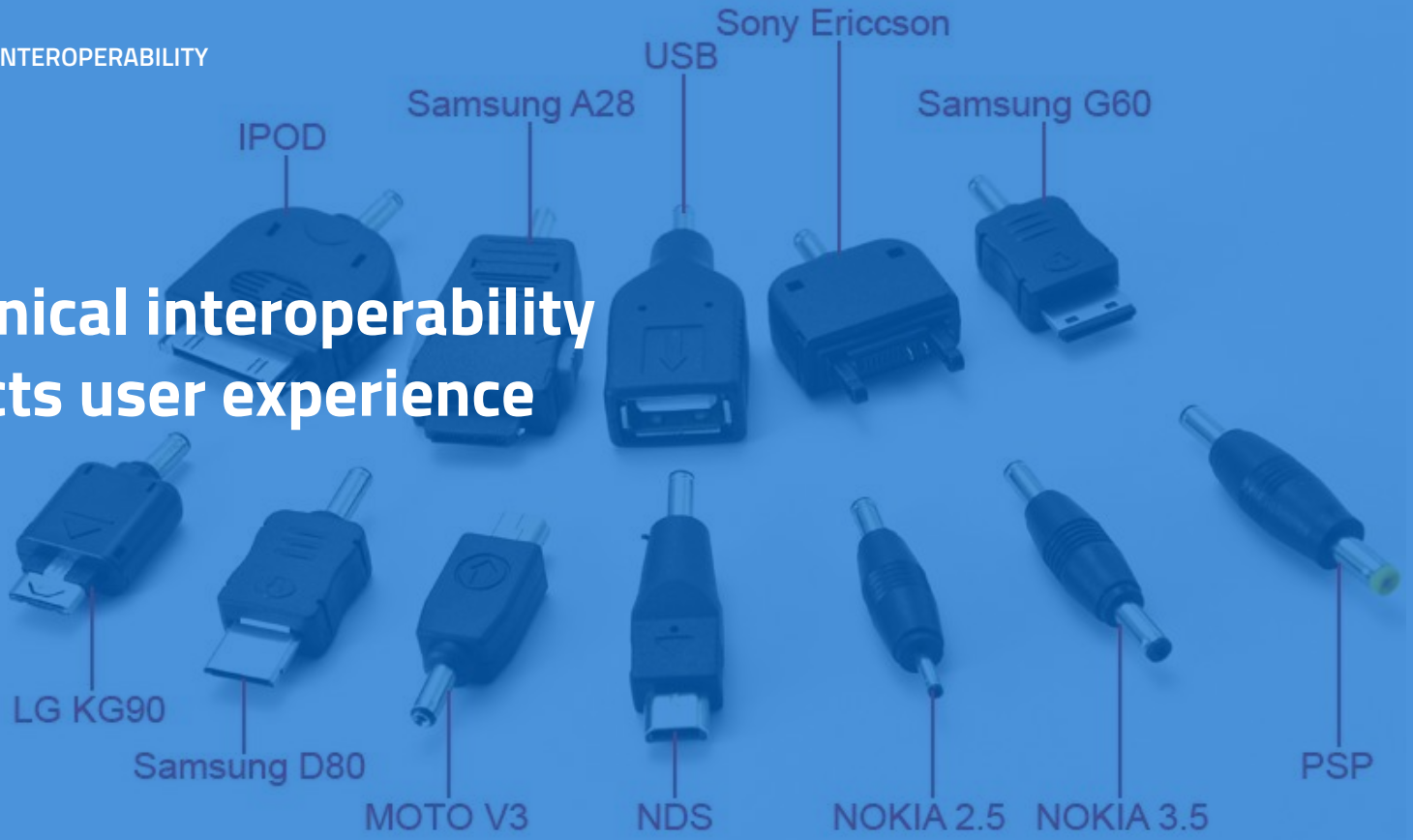
An Interoperability Framework for Public Services should be:

- 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

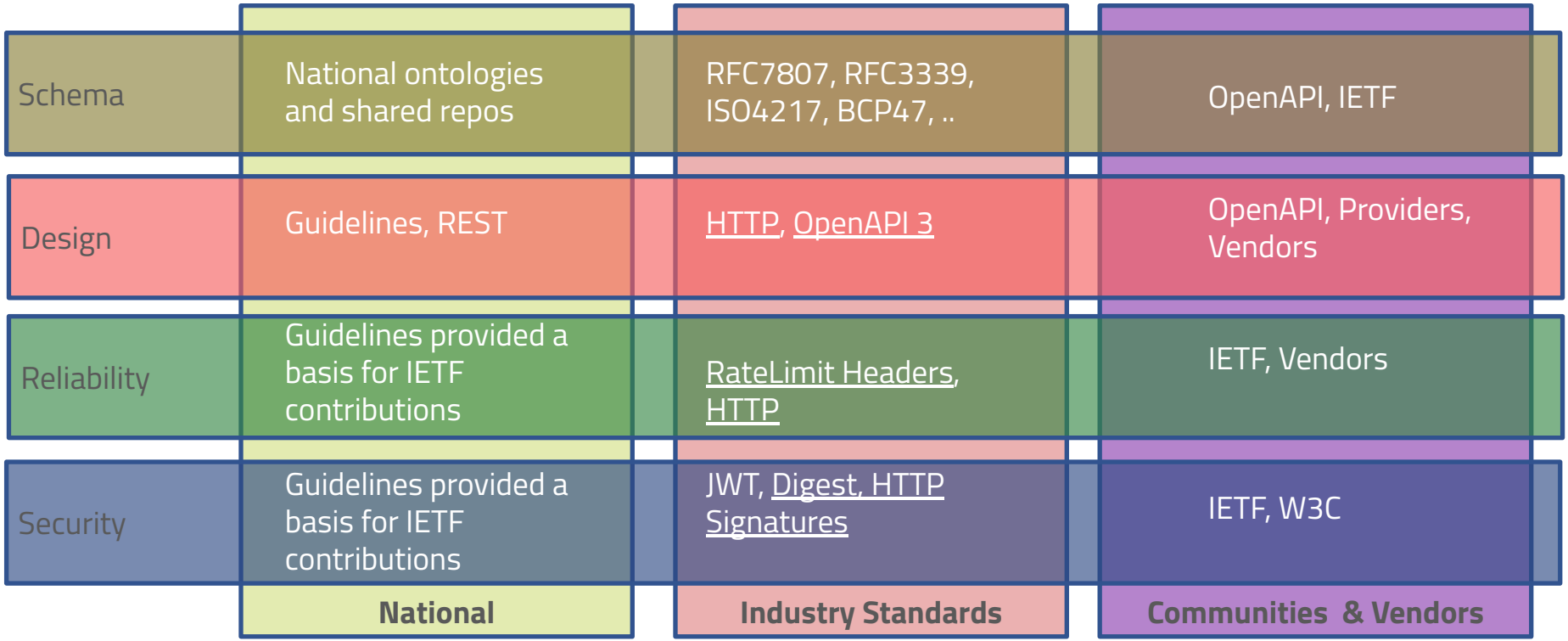
Public sector should:

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

Technical interoperability affects user experience



ADOPTING AND PROPOSING STANDARDS: AN EXCERPT



We joined the underlined spec/workgroups

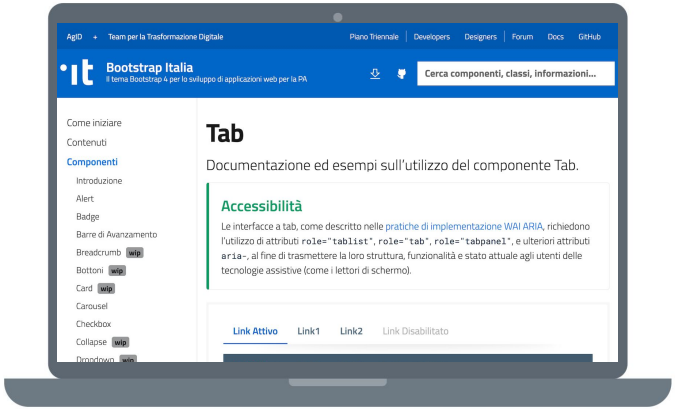
TEMPLATE SCHEDA 3

STATO

Piattaforma
abilitatrice all'accesso
a servizi pubblici e
privati, fisici e digitali

CITTADINI

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



TEAM PER LA
TRASFORMAZIONE
DIGITALE

ICONE VARIE