How much REST do you need?

International PHP Conference 2016

Kore Nordmann (@koredn)

1st July 2016

Hi, I’m Kore (@koredn)

Copyright Qafoo GmbH; All Rights Reserved

Isn’t It Just HTTP?

```
GET /jobs/23 HTTP/1.1
Host: api.qafoo.com
Accept: application/prs.com.qafoo.job+xml; version="2"
Authorization: v2039tkgsdgjr0wu4tpoesrig23itgesg

HTTP/1.1 200 OK
Content-Type: application/prs.com.qafoo.job+xml; version="2"; charset=UTF-8
ETag: "574295e8-297c"

<?xml version="1.0"?>
<job xmlns="urn:prs.com.qafoo.job"
     xmlns:atom="http://www.w3.org/2005/Atom">
     <!-- ... -->
     <atom:link
          rel="urn:prs.com.qafoo.job-assignments"
          type="application/prs.com.qafoo.job-assignment-list+xml"
          href="/jobs/23/assignments" />
     <!-- ... -->
</job>
```

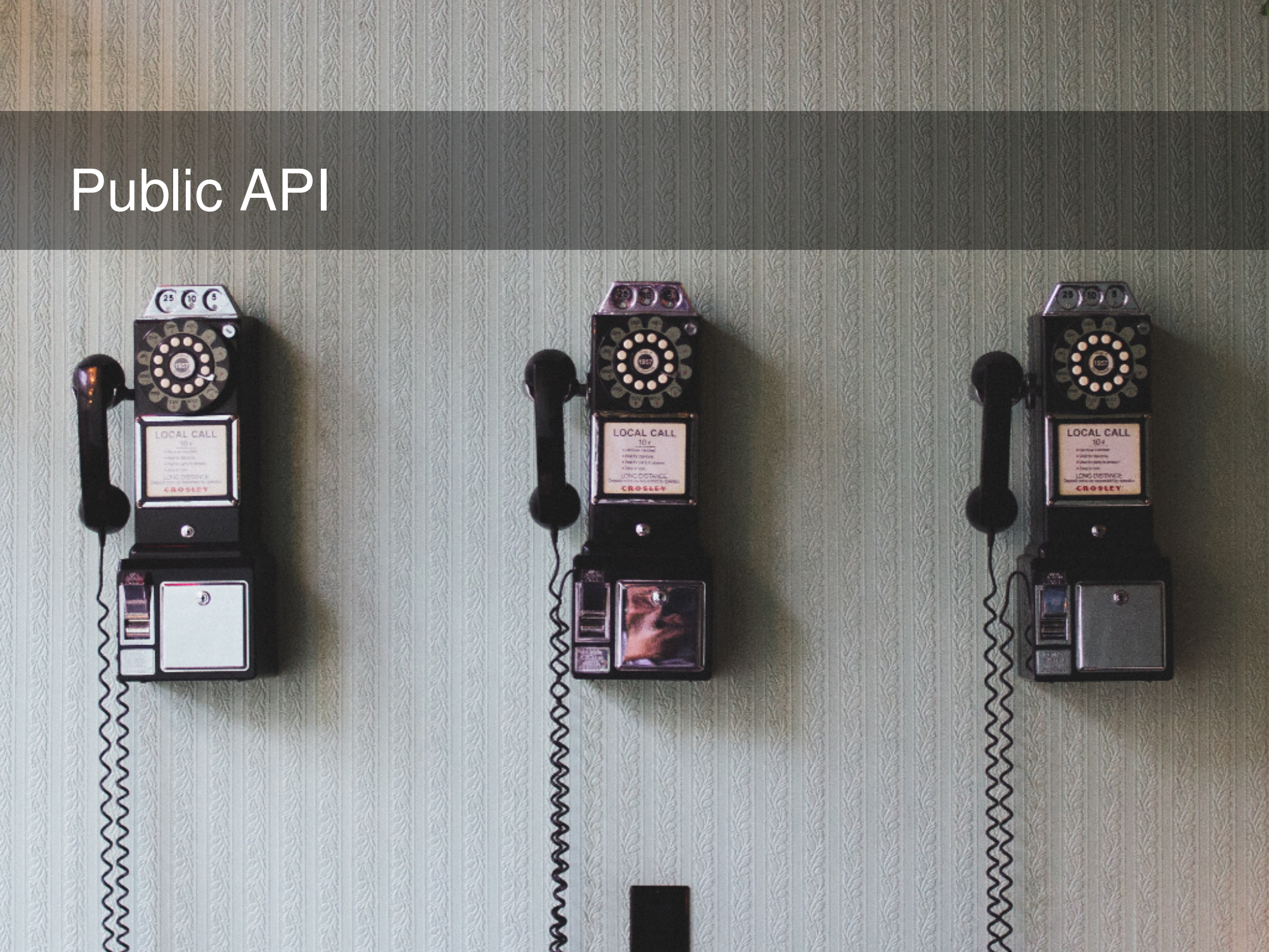

Copyright Qafoo GmbH; All Rights Reserved


REST(ful)

Different Levels of RESTfulness


Tradeoffs

Public API



Different Audiences

Many Different Constraints

HTTP Methods & URIs

```
1  GET /jobs/23 HTTP/1.1
2  Host: api.qafoo.com
3  Accept: application/prs.com.qafoo.job+xml; version="2"
4  Authorization: v2039tkgsdgjr0wu4tpoesrig23itgesg
5
6  HTTP/1.1 200 OK
7  Content-Type: application/prs.com.qafoo.job+xml; version="2"; charset=UTF-8
8  ETag: "574295e8-297c"
9
10 <?xml version="1.0"?>
11 <job xmlns="urn:prs.com.qafoo.job"
12      xmlns:atom="http://www.w3.org/2005/Atom">
13      <!-- ... -->
14      <atom:link
15          rel="urn:prs.com.qafoo.job-assignments"
16          type="application/prs.com.qafoo.job-assignment-list+xml"
17          href="/jobs/23/assignments" />
18      <!-- ... -->
19 </job>
```


Copyright Qafoo GmbH; All Rights Reserved

HTTP Methods

- **GET**
- HEAD
- OPTIONS
- TRACE
- **POST**
- **PUT**
- **DELETE**
- . . .

Copyright Qafoo GmbH; All Rights Reserved

URIs

- Collection
- Resource
- Query string to specify view parameters

```
/jobs
/jobs?count=10
/jobs/23
/jobs/23.xml
/jobs/23?format=xml
```


Copyright Qafoo GmbH; All Rights Reserved

Levels

- Use properly – nothing to trade in
- Stick to HTTP method properties!

Copyright Qafoo GmbH; All Rights Reserved

Media Types

```
GET /jobs HTTP/1.1
Host: api.qafoo.com
Accept: application/prs.com.qafoo.job-list+xml; version="2"
Authorization: v2039tkgsdgjr0wu4tpoesrig23itgesg

HTTP/1.1 200 OK
Content-Type: application/prs.com.qafoo.job-list+xml; version="2"; charset=UTF-8
ETag: "574295e8-297c"

<?xml version="1.0"?>
<jobs xmlns="urn:prs.com.qafoo.job-list">
    <job xmlns="urn:prs.com.qafoo.job">
        <!-- ... -->
    </job>
    <job xmlns="urn:prs.com.qafoo.job" href="/jobs/23" />
    <!-- ... -->
</jobs>
```


Copyright Qafoo GmbH; All Rights Reserved

Media Types

- Describe types
- Ease automatic marshalling
- `prs` – personal use (non-public media types)

```
application/prs.com.qafoo.job+xml
```

- Can be used for content negotiation (versioning)

Copyright Qafoo GmbH; All Rights Reserved

Embedded Resources

- Reduce number of required requests for a data set
- Can be problematic together with caching

```
<?xml version="1.0"?>
<jobs xmlns="urn:prs.com.qafoo.job-list">
    <job xmlns="urn:prs.com.qafoo.job">
        <!-- ... -->
    </job>
    <job xmlns="urn:prs.com.qafoo.job" href="/
        jobs/23" />
    <!-- ... -->
</jobs>
```


Copyright Qafoo GmbH; All Rights Reserved

Levels

- Media Types
  - Use for public APIs and enterprise APIs
  - Can help marshalling even for internal APIs
- Embedded Resources
  - Try not to use together with caching

Copyright Qafoo GmbH; All Rights Reserved

HATEOAS

```
GET /jobs/23 HTTP/1.1
Host: api.qafoo.com
Accept: application/prs.com.qafoo.job+xml; version="2"
Authorization: v2039tkgsdgjr0wu4tpoesrig23itgesg

HTTP/1.1 200 OK
Content-Type: application/prs.com.qafoo.job+xml; version="2"; charset=UTF-8
ETag: "574295e8-297c"

<?xml version="1.0"?>
<job xmlns="urn:prs.com.qafoo.job"
    xmlns:atom="http://www.w3.org/2005/Atom">
    <!-- ... -->
    <atom:link
        rel="urn:prs.com.qafoo.job-assignments"
        type="application/prs.com.qafoo.job-assignment-list+xml"
        href="/jobs/23/assignments" />
    <!-- ... -->
</job>
```


Copyright Qafoo GmbH; All Rights Reserved

HATEOAS

- Provide clients with actions on resources
  - Clients seldomly implement autodiscovery
- Commonly used for possible state transitions
  - Sematics (`rel`) not clearly defined
- Inline documentation

Copyright Qafoo GmbH; All Rights Reserved

Levels

- Use for workflow engines
- Use in evolving long-term projects (enterprise)

Copyright Qafoo GmbH; All Rights Reserved

Versioning

```
GET /jobs/23 HTTP/1.1
Host: api.qafoo.com
Accept: application/prs.com.qafoo.job+xml; version="2"
Authorization: v2039tkgsdgjr0wu4tpoesrig23itgesg

HTTP/1.1 200 OK
Content-Type: application/prs.com.qafoo.job+xml; version="2"; charset=UTF-8
ETag: "574295e8-297c"

<?xml version="1.0"?>
<job xmlns="urn:prs.com.qafoo.job"
     xmlns:atom="http://www.w3.org/2005/Atom">
     <!-- ... -->
     <atom:link
          rel="urn:prs.com.qafoo.job-assignments"
          type="application/prs.com.qafoo.job-assignment-list+xml"
          href="/jobs/23/assignments" />
     <!-- ... -->
</job>
```


Copyright Qafoo GmbH; All Rights Reserved

Versioning

- Media Type based versioning
  - Indicate new versions of resource / collection formats
  - Clients & server must be able to handle them
- URL based versioning
  - Only use for structurally changed APIs (rewrites)

```
1 /jobs/23 (Accept: application/prs.com.qafoo.job-v2+xml)
2 /jobs/23 (Accept: application/prs.com.qafoo.job+xml;
      version="2")
3 /v2/jobs/23 (Accept: */*)
```


Copyright Qafoo GmbH; All Rights Reserved

Levels

- Private APIs: Do not use, just adapt
- Public APIs: Try not to use, clients will misbehave
- Enterprise APIs: Use, but with foresightedness

Copyright Qafoo GmbH; All Rights Reserved

Caching

```
1  GET /jobs/23 HTTP/1.1
2  Host: api.qafoo.com
3  Accept: application/prs.com.qafoo.job+xml; version="2"
4  Authorization: v2039tkgsdgjr0wu4tpoesrig23itgesg
5
6  HTTP/1.1 200 OK
7  Content-Type: application/prs.com.qafoo.job+xml; version="2"; charset=UTF-8
8  ETag: "574295e8-297c"
9
10 <?xml version="1.0"?>
11 <job xmlns="urn:prs.com.qafoo.job"
12      xmlns:atom="http://www.w3.org/2005/Atom">
13      <!-- ... -->
14      <atom:link
15          rel="urn:prs.com.qafoo.job-assignments"
16          type="application/prs.com.qafoo.job-assignment-list+xml"
17          href="/jobs/23/assignments" />
18      <!-- ... -->
19 </job>
```


Copyright Qafoo GmbH; All Rights Reserved

Caching Is Hard

Cache Expiry

- `Expires: <date>`
- `Cache-Control:`
  - `public` / `private`
  - `no-cache` / `no-store`
  - `max-age=<seconds>` / `s-maxage=<seconds>`
- Attention: Expiry heuristics

Copyright Qafoo GmbH; All Rights Reserved

Validation

- Origin server
  - `ETag: <hash>`
  - `Last-Modified: <date>`
- Client
  - `If-None-Match: <hash>`
  - `If-Modified-Since: <date>`
- Optimistic locking (MVCC)
- Mind embedded resources

Copyright Qafoo GmbH; All Rights Reserved

Levels

- Private-API: `Cache-Control: no-cache, no-store, max-age=0`
- Public-API: If accessed by browsers: Do all the complex stuff
- Enterprise-API: `Cache-Control: no-cache, no-store, max-age=0`

Copyright Qafoo GmbH; All Rights Reserved

Authentication / Authorization

```
GET /jobs/23 HTTP/1.1
Host: api.qafoo.com
Accept: application/prs.com.qafoo.job+xml; version="2"
Authorization: v2039tkgsdgjr0wu4tpoesrig23itgesg

HTTP/1.1 200 OK
Content-Type: application/prs.com.qafoo.job+xml; version="2"; charset=UTF-8
ETag: "574295e8-297c"

<?xml version="1.0"?>
<job xmlns="urn:prs.com.qafoo.job"
     xmlns:atom="http://www.w3.org/2005/Atom">
     <!-- ... -->
     <atom:link
          rel="urn:prs.com.qafoo.job-assignments"
          type="application/prs.com.qafoo.job-assignment-list+xml"
          href="/jobs/23/assignments" />
     <!-- ... -->
</job>
```


Copyright Qafoo GmbH; All Rights Reserved

Basic / Digest Auth

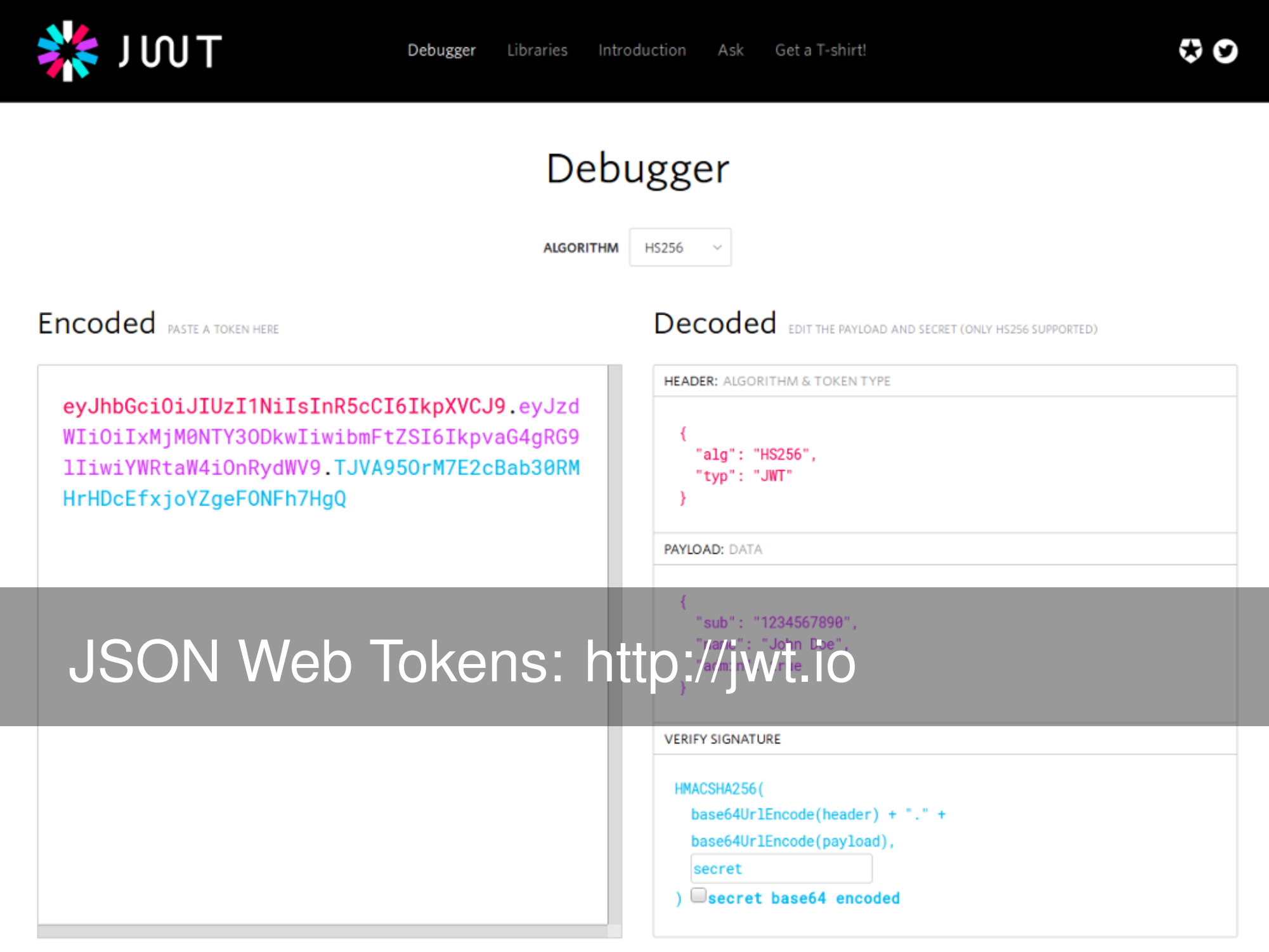
- HTTP default auth methods
- Basic
  - → Some request
  - ← `401 WWW-Authenticate:  Basic realm="My API"`
  - → `Authorization:  Basic dG9ieTpxYWZvbw==`
- Digest
  - Hashing with server provided nounce
  - Slightly more secure, since no clear text password
- Use HTTPS with Basic and Digest!

Copyright Qafoo GmbH; All Rights Reserved

API Key

- Authenticate an application by pre-shared key
- Use HMAC to verify keys
- Custom `WWW-Authenticate` / `Authorization` format or a custom header

Copyright Qafoo GmbH; All Rights Reserved



JSON Web Tokens: http://jwt.io

OAuth2

- Authenticate users 3rd party apps
  - e.g. Twitter / Facebook / . . .
- Allows fine-grained permission system
  - Read personal information
  - Read friend list
  - Post as user
  - . . .
- `http://oauth.net/2/`

Copyright Qafoo GmbH; All Rights Reserved

Levels

Always use HTTPS

- Private-API: Digest or simple Tokens are OK
- Public-API: JWT, custom Tokens or OAuth2
- Enterprise-API: JWT, custom Tokens or OAuth2

Copyright Qafoo GmbH; All Rights Reserved

Many Different Constraints

Choose Your Style

THANK YOU

Rent a quality expert
qafoo.com

Copyright Qafoo GmbH; All Rights Reserved