DevExpress

Using Secure WebAPI services from a JavaScript SPA

Don Wibier
Technical Evangelist /DEVEXPRESS
Microsoft MVP

donw@devexpress.com
@donwibier

Agenda

Using secure WebAPI

WEBAPI: what, why?

Create WebAPI Service

Consume WebAPI Service

Terms

WEBAPI

REST

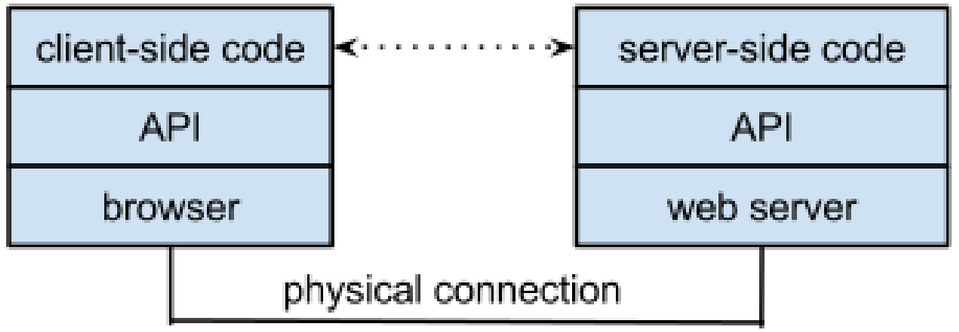
ENDPOINTS

JSON

OAUTH

Define

A web API is a subset of an application programming interface (API)

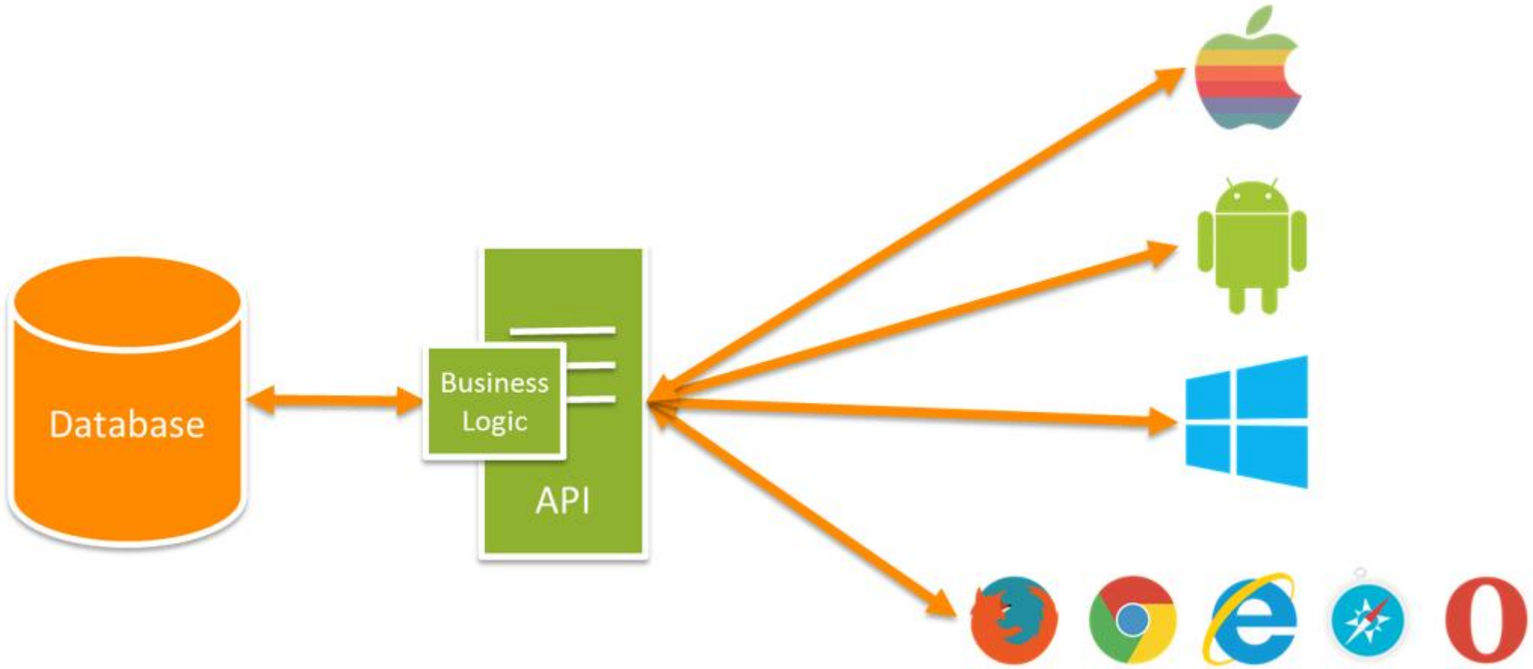


wikipedia.org

Define

Using secure WebAPI

API – Why?



blogs.msdn.com/b/martinkearn

REST & HTTP

Using secure WebAPI

RESTful API HTTP methods

Resource	GET	PUT	POST	DELETE
Collection URI, such as `http://api.example.com/resources/`	**List** the URIs and perhaps other details of the collection's members.	**Replace** the entire collection with another collection.	**Create** a new entry in the collection. The new entry's URI is assigned automatically and is usually returned by the operation.[10]	**Delete** the entire collection.
Element URI, such as `http://api.example.com/resources/item17`	**Retrieve** a representation of the addressed member of the collection, expressed in an appropriate Internet media type.	**Replace** the addressed member of the collection, or if it does not exist, **create** it.	Not generally used. Treat the addressed member as a collection in its own right and **create** a new entry in it.[10]	**Delete** the addressed member of the collection.

wikipedia.org

EndPoints

Using secure WebAPI

httpbin(1): HTTP Request & Response Service

Freely hosted in HTTP, HTTPS & EU flavors by Runscope

ENDPOINTS

/ This page.
/ip Returns Origin IP.
/user-agent Returns user-agent.
/headers Returns header dict.
/get Returns GET data.
/post Returns POST data.
/patch Returns PATCH data.
/put Returns PUT data.
/delete Returns DELETE data
/encoding/utf8 Returns page containing UTF-8 data.
/gzip Returns gzip-encoded data.
/deflate Returns deflate-encoded data.
/status/:code Returns given HTTP Status code.
/response-headers?key=val Returns given response headers.

httpbin.org

OAuth

Using secure WebAPI

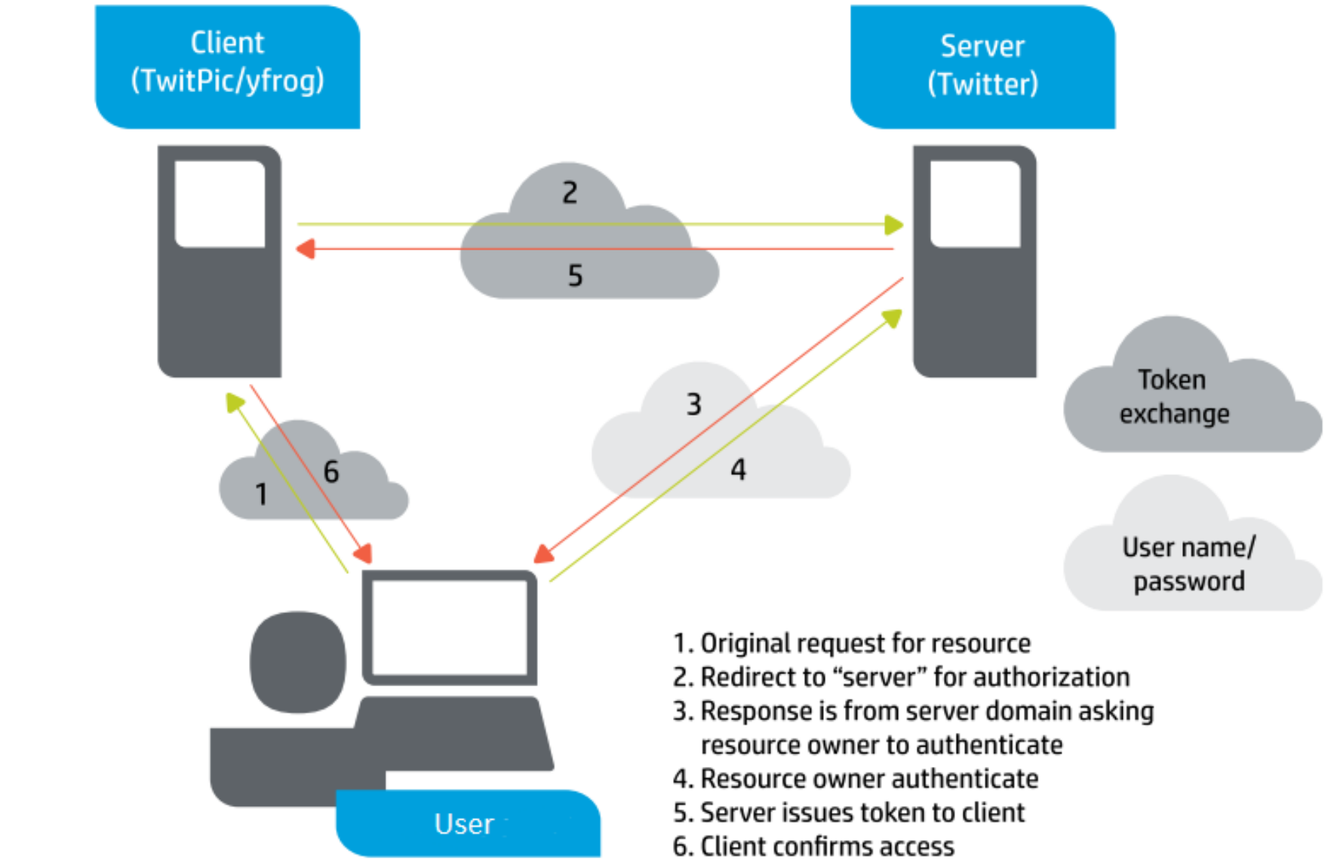


Figure 1 OAuth flow diagram

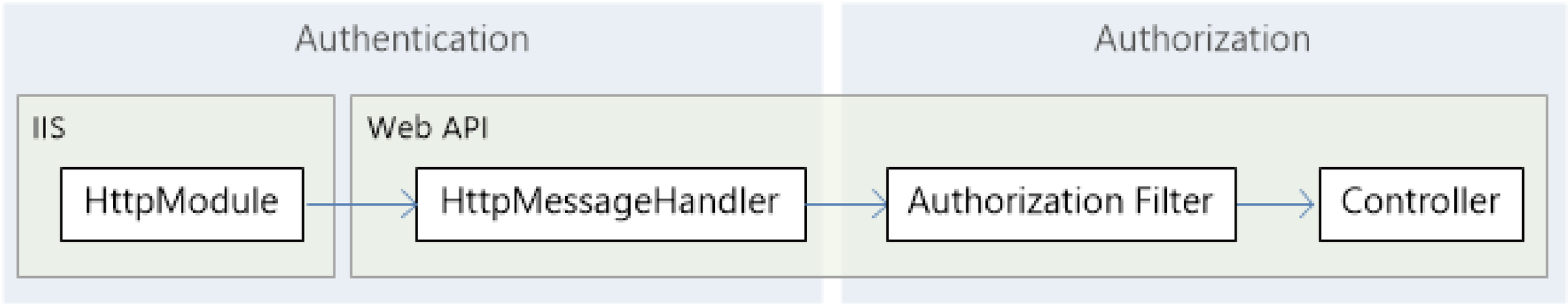
community.hpe.com

DevExpress®

Authentication

Using secure WebAPI

And Authorization



Create a
Secure
WebAPI
Web Service

How to secure…

1. Decorating the WebAPI Controller

- Use the [Authorize(..)] attribute

2. Decorating individual Action Methods

- Exclusions on Controller attributes ([OverrideAuthentication(..)], [AllowAnonymous])
- Individual methods to be secure ([Authorize(..)])

Authorize

AllowAnonymous ?

```
[Authorize]
public class ValuesController : ApiController
{
    [AllowAnonymous]
    public HttpResponseMessage Get() { ... }

    public HttpResponseMessage Post() { ... }
}
```

Authorize

Using secure WebAPI

Restrict by

```
// Restrict by user:
[Authorize(Users="Alice,Bob")]
public class ValuesController : ApiController
{
}

// Restrict by role:
[Authorize(Roles="Administrators")]
public class ValuesController : ApiController
{
}
```

Application/Client types

Same-Domain

- Web APIs and clients live in the same domain
  - all security settings inherited from web host

Cross-Domain

- Web APIs and clients live in different domains
  - native apps (desktop, mobile)
  - client side JavaScript code (browser)
- Web API specific security settings

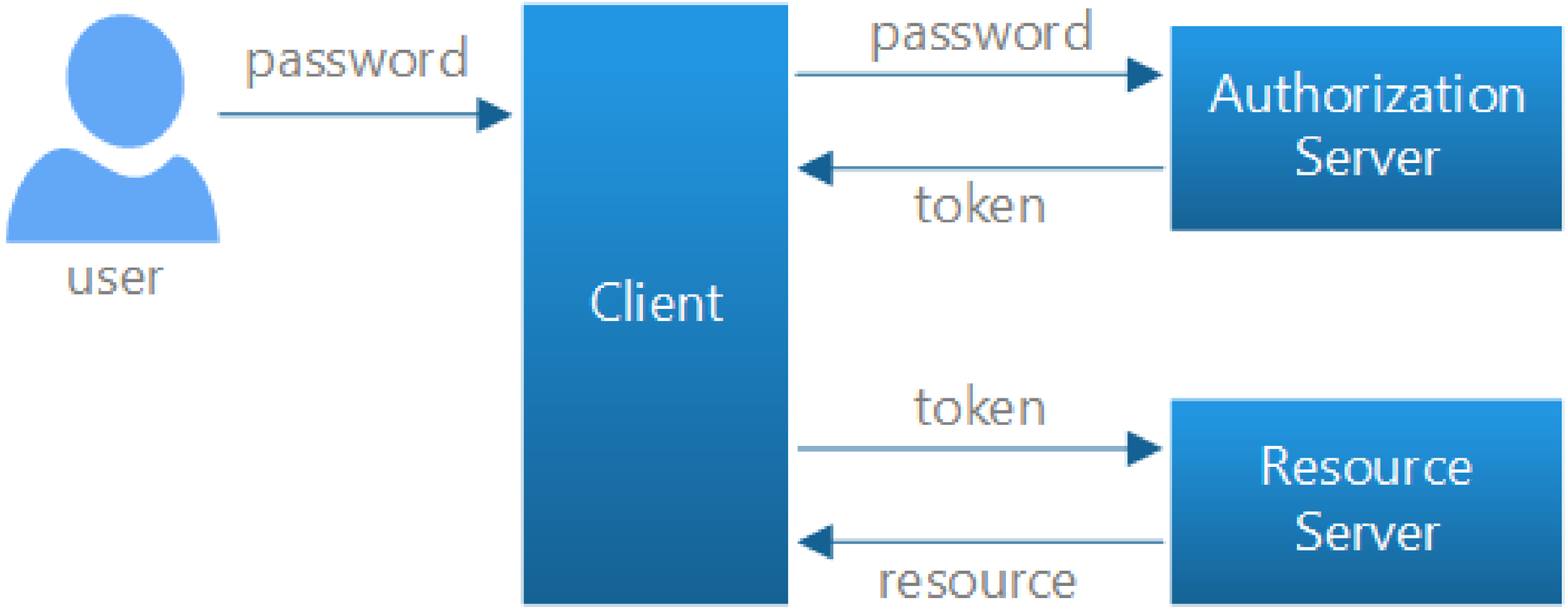
Using secure WebAPI

Consume
Secure
WebAPI
Web Service

Credential Flow

Using secure WebAPI

Local login



Client side

Send authenticated request

```
// If we already have a bearer token, set the Authorization header.
var token = sessionStorage.getItem(tokenKey);
var headers = {};
if (token) {
    headers.Authorization = 'Bearer ' + token;
}

$.ajax({
    type: 'GET',
    url: 'api/values/1',
    headers: headers
}).done(function (data) {
    self.result(data);
}).fail(showError);
```

Best Practices

Use SSL

IIS

IIS Express

Controller

Action [RequireHttps]

dxpr.es/api-ssl

Using secure WebAPI

blog.cloudflare.com

Best Practices

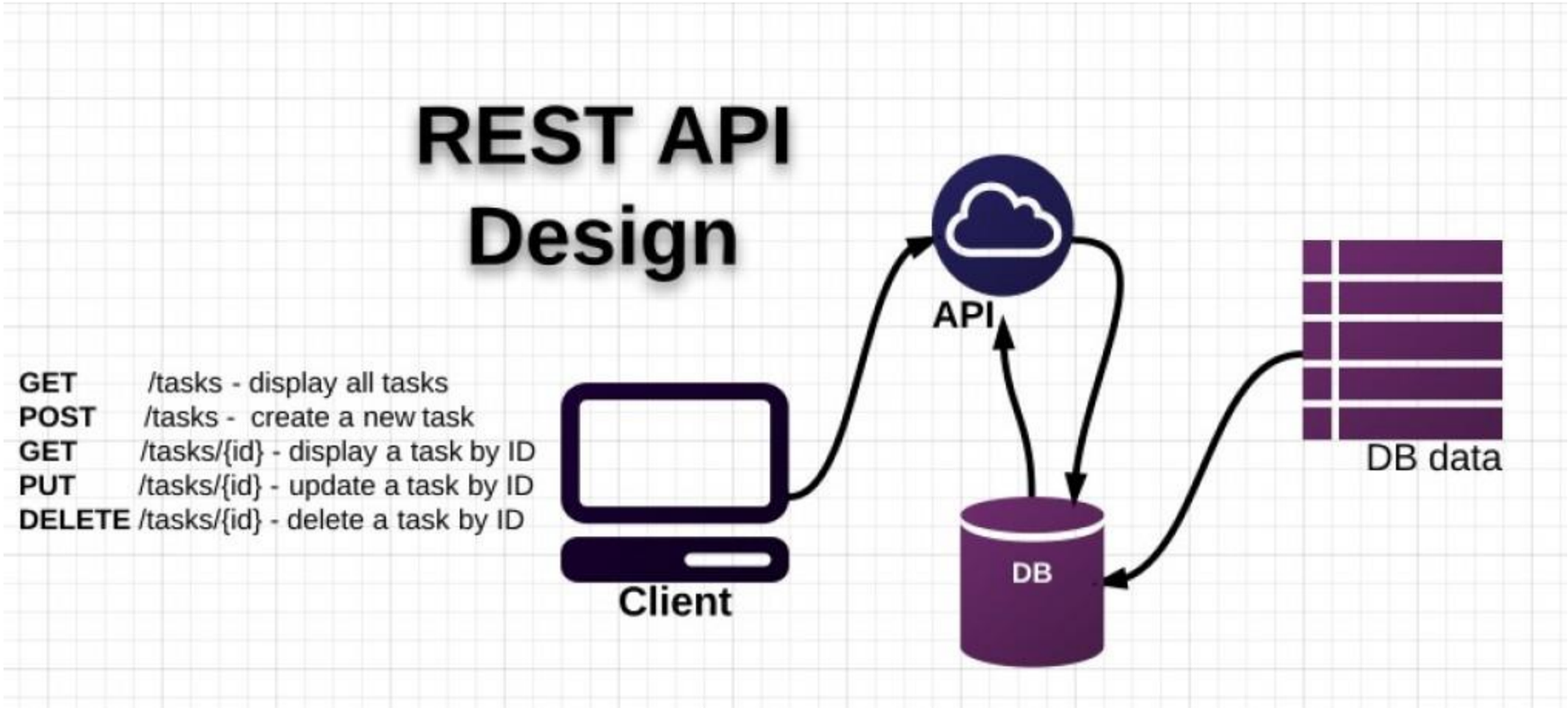
Using secure WebAPI

KISS

[API design guidance]

[RESTful API design]

[Pragmatic RESTful API]



maxoffsky.com

DevExpress

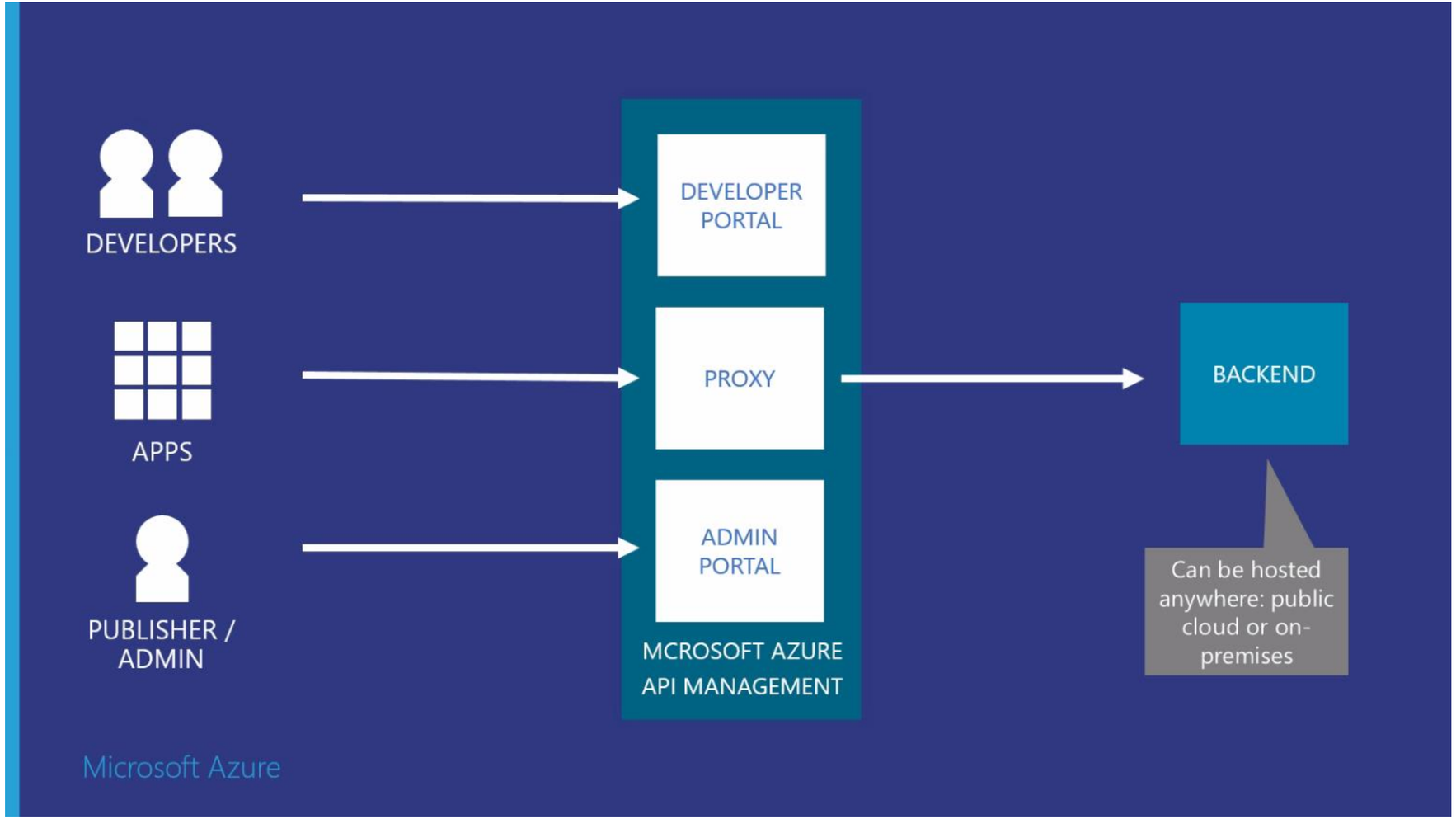
Best Practices

Using secure WebAPI

Cloud

API Management

Azure, apigee, etc.

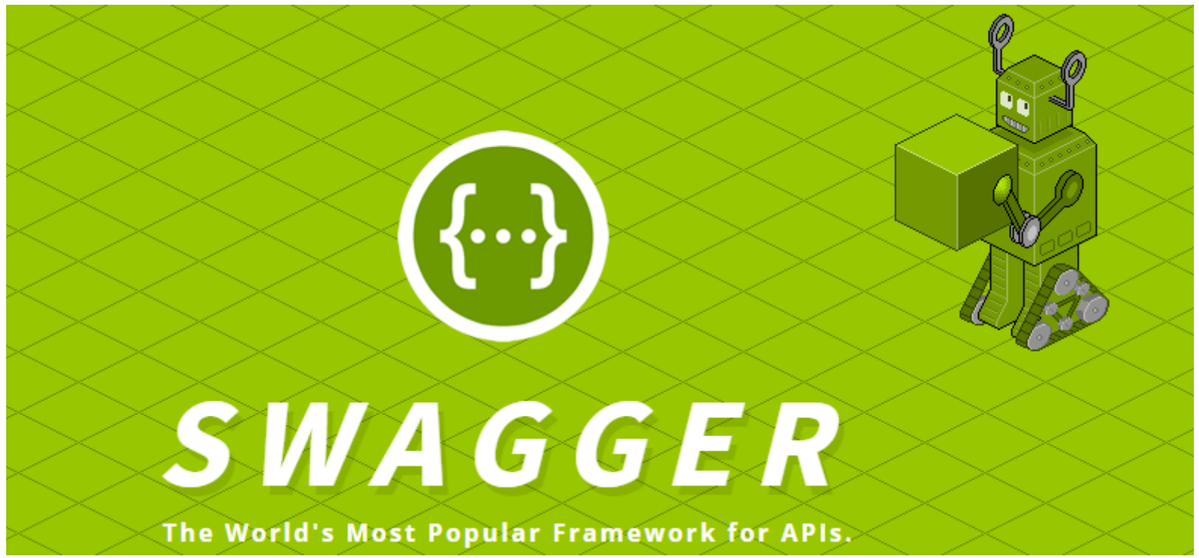


Tips

Go Public?

Metadata – Swagger.io

Programmableweb.com



ProgrammableWeb

Thank You!

donw@devexpress.com
@donwibier