Miroslav Holec

KONZULTANT PRO .NET

Nejčastější chyby v návrhu REST API

prezentace a dema

www.**wug.cz**

dotnetnews.cz & miroslavholec.cz

mirek@miroslavholec.cz

Agenda

- nejčastější oblasti, ve kterých selhává návrh API
- seznámení s každou oblastí a zásadami
- konkrétní příklady chyb v návrhu

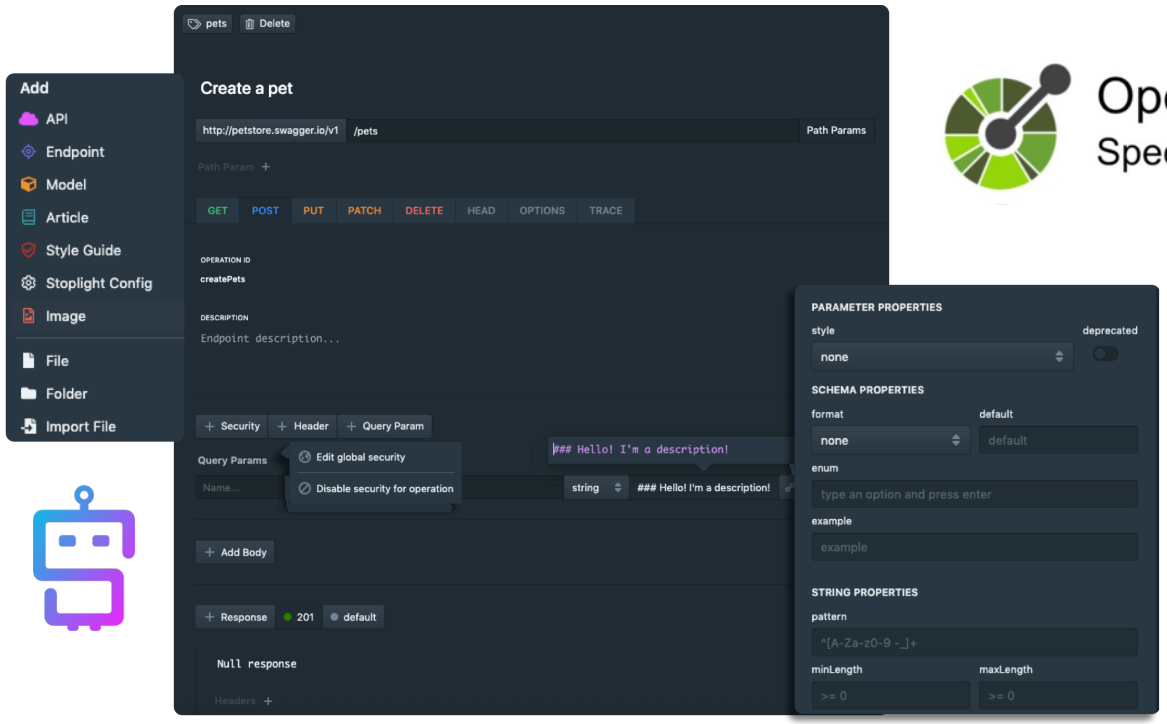
Dnes neřešíme detaily typu podoba struktur, URL, atd... doporučuji:

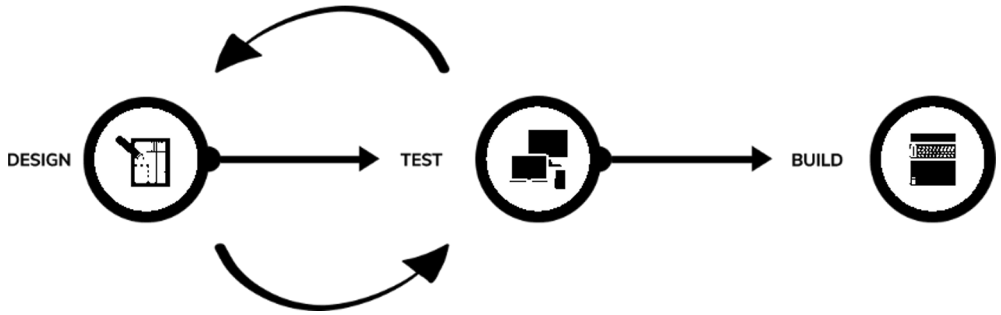
RESTAPI.CZ

- průvodce pro návrh REST API (endpointy, struktury, standardy, pravidla)
- metodika Design First (metodika návrhu, specifikace rozhraní)

Design First

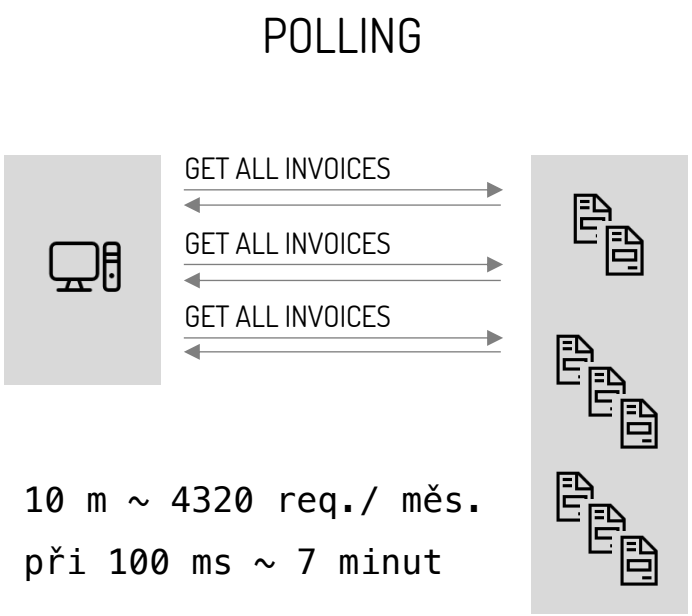
- **pro každou DB tabulku se udělá controller a operace GET, PUT, POST, DELETE, ...**
- **endpointy se programují neorganizovaně dle potřeby < bez celkového pohledu na systém >**
- **příliš univerzální API pro příliš specifické případy užití**

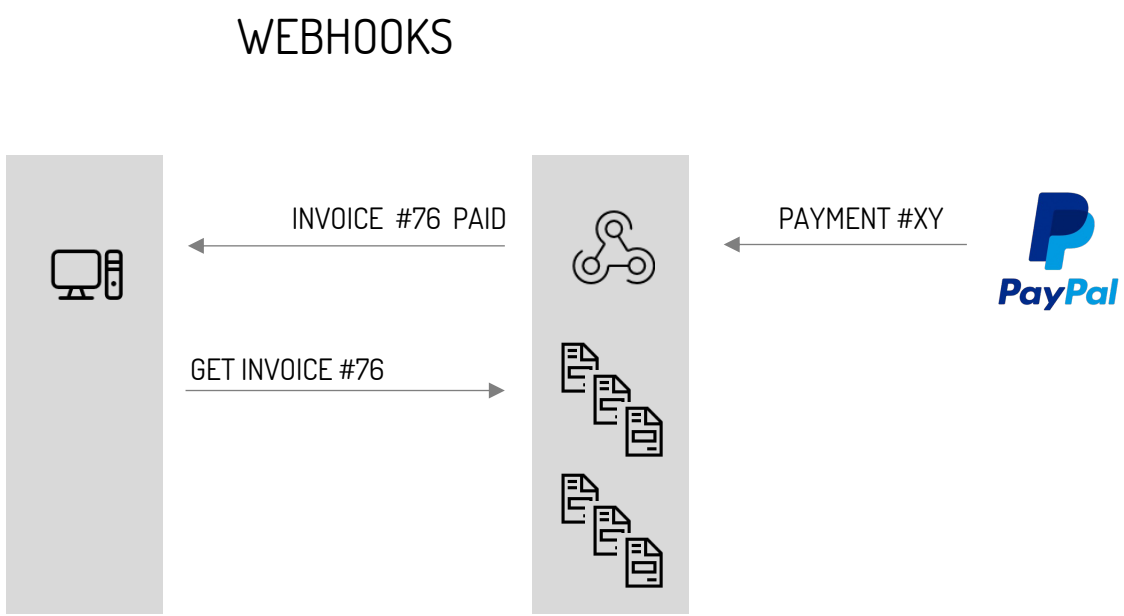




Webhooks

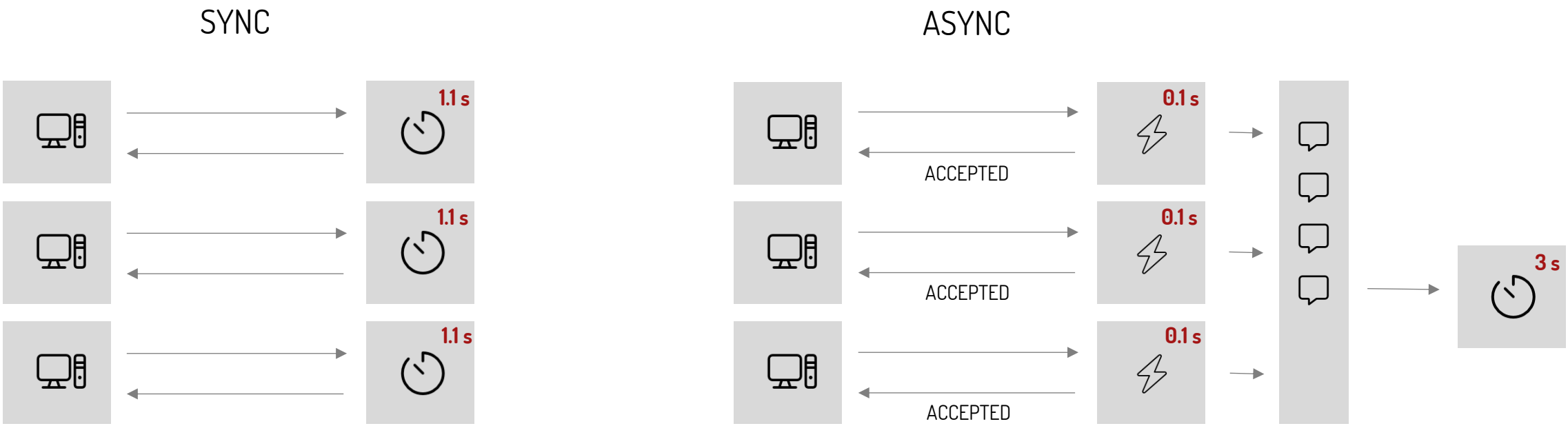
- **zcela chybí podpora webhooks**
- **webhooks neimplementují retry policy**
- **zasílání citlivých dat, nezabezpečená komunikace, umožnit IP whitelisting**
- **chybí konfigurace událostí, které se zasílají**





Asynchronní endpointy

- **všechny endpointy jsou synchronní < klient čeká na odpověď >**
- **asynchronní endpoint má za sebou pomalou implementaci**
- **chybí základní validace vstupů**
- **implementace není idempotentní**



HTTP Caching

- **chybí podpora HTTP hlaviček pro cachování**
- **je implementována jen statická cache přes Max-Age**

STATIC CACHING

Age:	157760
Cache-Control:	max-age=604800, must-revalidate

max-age
no-cache
no-store
must-revalidate
private
public

CONDITIONAL HEADERS

Etag:	"uc/tOfGRffWra0pxg2UlJw=="
Expires:	Wed, 26 Feb 2025 13:24:58 GMT
Last-Modified:	Thu, 22 Feb 2024 15:48:05 GMT

etag

- hash, třeba sha1
- versionuid

Chybové struktury

- **API vrací ve všech případech status code 200**
- **chybové struktury nejsou jednotné < každý status code má jinou >**
- **ignoruje se HTTP hlavička Accept**
- **nejednotná naming konvence pro properties**

```
{
   "errors": {
      "firstname": [ "required field" ],
      "lastname": [ "required field" ]
   },
   "type": "https://www.restapi.cz/probs/validation-problem-details",
   "title": "Validation Failed",
   "status": 400
}
```

Konzistentnost rozhraní

- **ve filtrování (query params) má znak “=„ různý význam (contains, equals)**
- **volba nevhodných jednotek** (minuty vs. sekundy, kilometry vs. metry)
- **místo standardů se používá obecný text** (doba trvání, GPS, telefonní čísla)
- **nejednotné názvy vlastností** (dateFrom, dateStart, startDate, from)

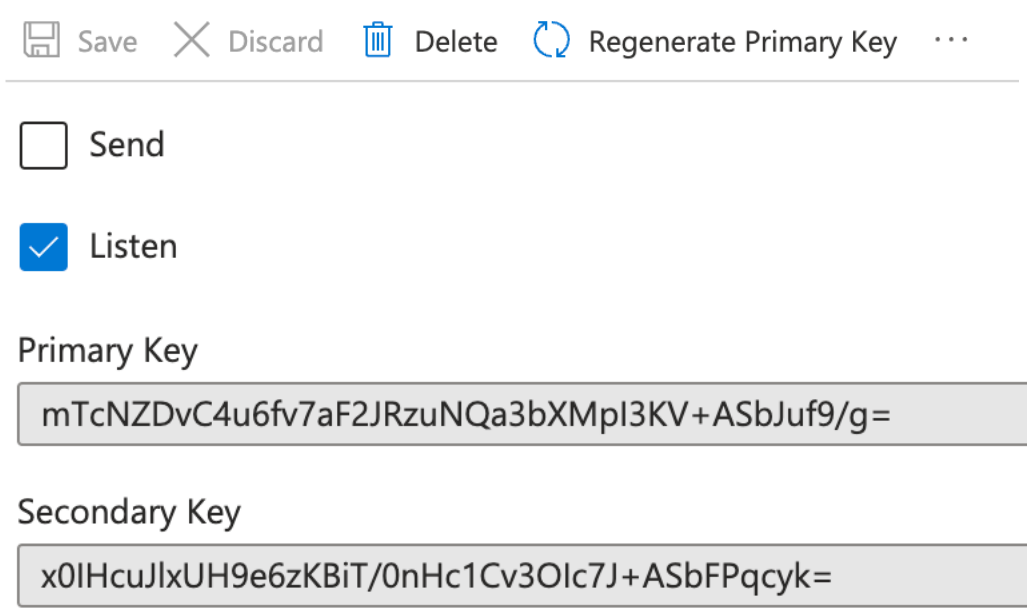
```
GET    products?titleCt=hrnek

"dateFrom"    : "2019-01-01T12:45:00+0500",
"duration"    : "PT1H",
"latitude"    : 48.8566,
"longitude"    : 13.1766,
"phoneNumber" : "+420123456789",
"currency"    : "EUR",
"vatRate"     : 0.21
```

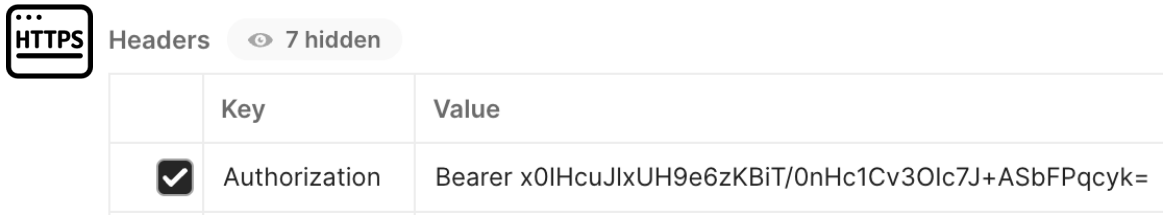
Průvodce designem (formát dat)

www.odkaz.me/frm

API Key autentizace

- **klíče mají nekonečnou platnost a / nebo je nelze invalidovat**
- **chybí podpora sekundárního klíče**
- **nešikovná implementace přes middleware v .NETu**





JWT tokeny

- **obsahují citlivé informace**
- **jsou hraničně velké a obsahují mnoho informací, které se v čase mění**
- **mají extrémně dlouhou platnost - nepochopení principu fungování**

```
{
   "alg": "HS256",
   "typ": "JWT"
}
```

```
{
   "sub": "1234",
   "name": "john"
}
```

```
HMACSHA256(
base64UrlEncode(header) + "." +
base64UrlEncode(payload),
secret)
```

BASE64

```
eyJhbGciOiJIUzI1NiIsInR5cCI6IkpXVCJ9.
eyJzdWIiOiIxMjM0NTY3ODkwIiwibmFtZSI6IkpvaG4
gRG9lIiwiaXNTb2NpYWwiOnRydWV9.
4pcPyMD09olPSyXnrXCjTwXyr4BsezdI1AVTmud2fU4
```

claims
RFC 7519 – JSON Web Token
OpenID Connect
RFC 8225 – pers. assertion token
RFC 8417 – security event token
... nebo vlastní claims

Performace na backendu

- **převládají blokující volání, chybí implementace async & await**
- **chybí podpora abort requestů a cancellation tokenů**
- **vůbec se nepoužívá serverová cache**
- **preference pomalých úložišť jako relační databáze**
- **používání Newtonsoft.Json místo System.Text.Json**
- **neefektivní autentizace, například access tokeny místo JWT**
- **relační mappery jako entity framework < jsou špatně použité >**
- **spoléhání na relační mappery, chybějící optimalizace databáze, indexy**

Další technologie

gRPC – „g“ remote procedure call

- tlak na vysoký výkon, rychlá komunikace, real-time výměna dat a importy, microservices
- contract first, univerzální – protobuf, skvělá podpora v .NET

GraphQL – Graph Query Language

- flexibilní dotazy na straně klienta, specifikace požadovaných dat pro různorodá UI
- vede ke snížení počtu requestů, velmi dobrá podpora v .NET

AMQP – Advanced Message Queuing Protocol

- výměna zpráv mezi systémy, vysoké nároky na výkon, zabezpečení a spolehlivost doručení zpráv
- typická implementace například Service Bus v Azure nebo RabbitMQ

SignalR – realtime komunikace a push notifikace

Miroslav Holec

KONZULTANT

mirek@miroslavholec.cz

miroslavholec.cz

Rozšířená verze přednášky a ukázky .NET kódu webhooks, async zpracování, cachování a dalších témat najdete během března na

miroslavholec.cz/premium