Marco De Sanctis
Developer Technologies MVP
info@marcodesanctis.it - @crad77

Building SaaS applications with ASP.NET Core and Azure

Our SaaS playground: enter Enterprise Chat

(a.k.a. "you want to build a Slack clone, but you can't design a website" ☺)

DEVELOPER .NET **DAYS**

Custom domains

Corporate SSO

Multi-tenancy

https://contoso.enterprisechat.co.uk/chatroom/5

Team contoso

Hello, test user!   Log out   About

🏠 Home

🔒 Default Contoso

🔒 SecretsHere!

Default Contoso

Kate 13/09/2022 14:28:13
Carl, we need to talk about that customer meeting

Carl 14/09/2022 20:13:32
Sure, what do you think?

Juliet 15/09/2022 09:32:24
Hey guys, don't use the public room for this, please! 😉

Kate 24/09/2022 13:33:16
Sorry!!! 🥳

Data Isolation

Before we proceed, one important caveat

What we are going to work on, is only

ONE POSSIBLE SOLUTION

Keeping data siloed: isolation strategies

Separate databases

Acme

Contoso

Fabrikam

Separate schemas

acme

contoso

fabrikam

Discriminator column

ChatRooms			
			acme
			acme
			contoso
			fabrikam

ChatMessages			
			fabrikam
			contoso
			contoso
			acme

✓

Ok, discriminator column, but how?!

```sql
SELECT *
FROM Rooms
WHERE CompanyID = 'acme'
```

What if you forget it?

ChatRooms		
		acme
		acme
		contoso
		fabrikam

SQL Server's Row Level Security

One possible option to have an "allow-list" approach
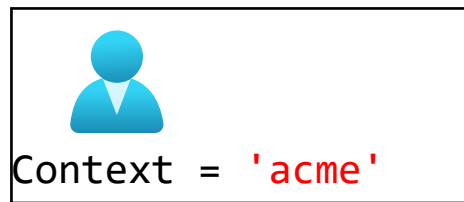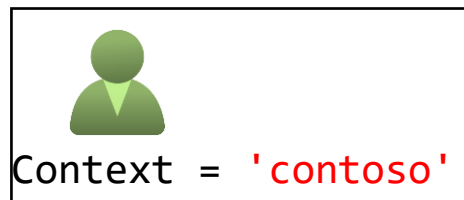
Demo

Discriminator column and Row-level security

Multi-tenant networking

*.enterprisechat.com

Key Vault

URL Rewrite requires a server-side component

Managed Identity

acme.enterprisechat.com

contoso.enterprisechat.com

*.enterprisechat.com

52.101.33.180

HTTPS

Listener

Rules

Rewrites

/*

Backend

/api/*

ui.azurewebsites.net?companyId=acme

UI

api.azurewebsites.net/api/acme/...

API

Application Gateway

DNS Zone

Public IP
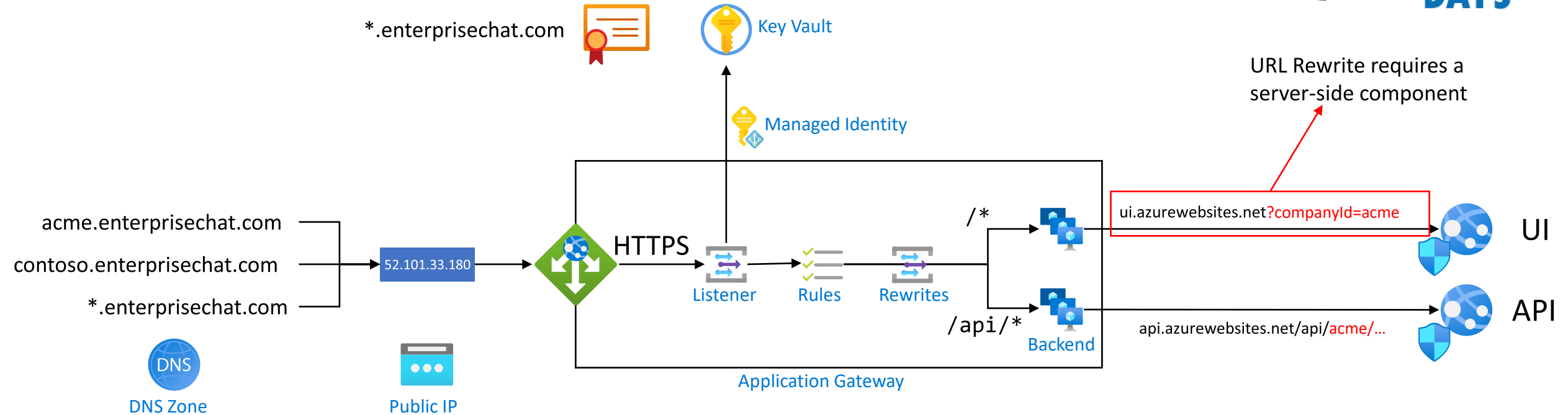
PREMIUM   Call 020 7084 1810 for buying assistance
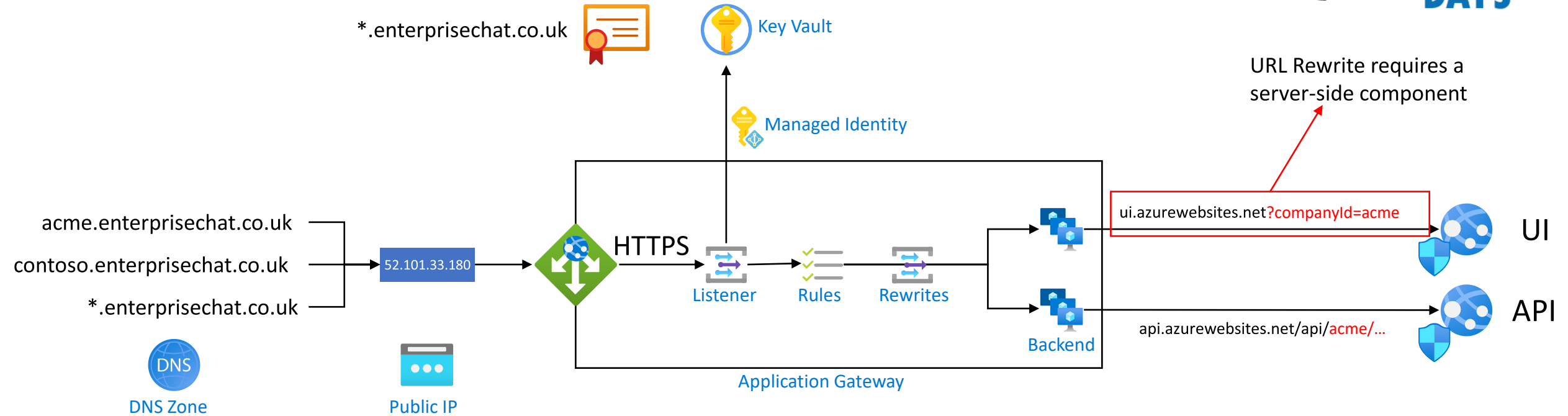
enterprisechat.com

£8,709

Buy now at this price or make offer to current owner.
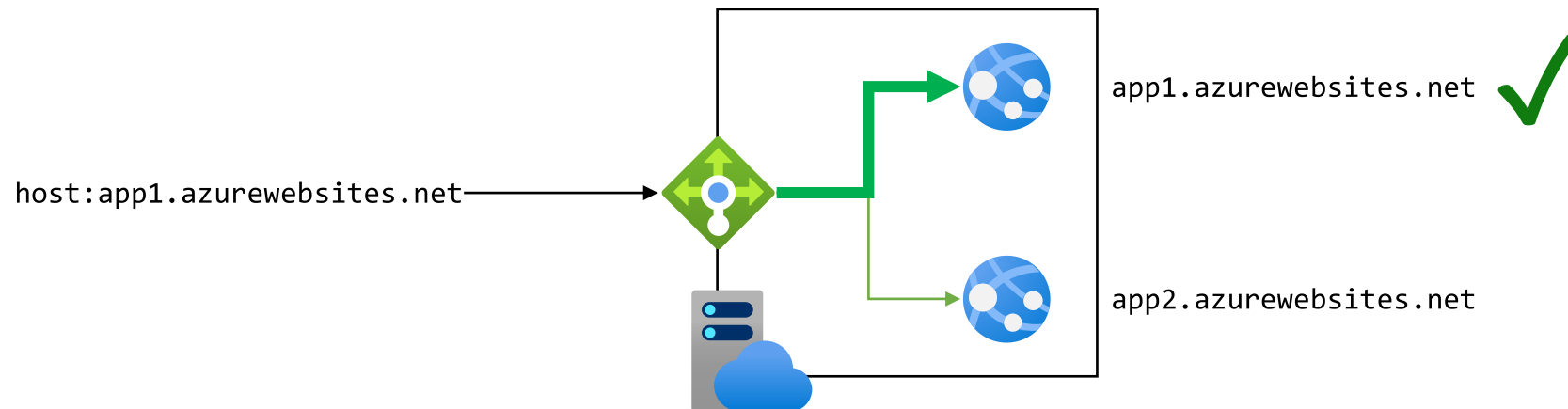
Get It   Learn More

Multi-tenant networking

*.enterprisechat.co.uk

Key Vault

Managed Identity

URL Rewrite requires a
server-side component

acme.enterprisechat.co.uk

contoso.enterprisechat.co.uk

*.enterprisechat.co.uk

52.101.33.180

HTTPS

Listener

Rules

Rewrites

Backend

Application Gateway

DNS Zone

Public IP

ui.azurewebsites.net?companyId=acme

UI

api.azurewebsites.net/api/acme/...

API

@DeveloperDaysPL

net.developerdays.pl

Demo

Azure delivery network

Beware of multi-site services like App Services

host:app1.azurewebsites.net

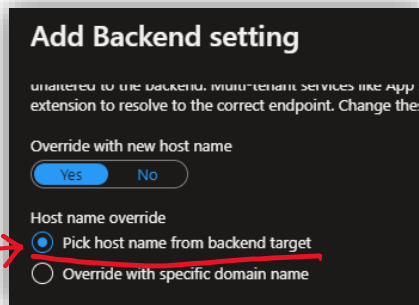app1.azurewebsites.net ✓

app2.azurewebsites.net

Beware of multi-site services like App Services

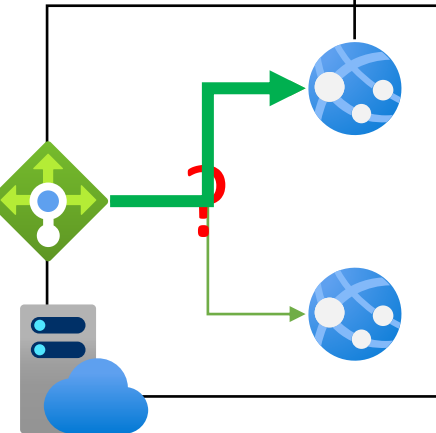

Sign in
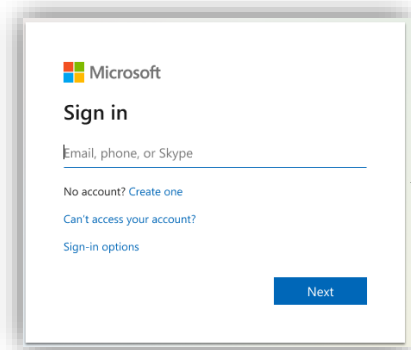
```
?returnUrl=contoso.enterprise...     ✓
?returnUrl=app1.azurewebsites.net    ✗
```

```
builder.Services
    .Configure<ForwardedHeadersOptions>(
{
    // ...
});

app.UseForwardedHeaders();
```

host:contoso.enterprisechat.com

```
host:contoso.enterprisechat
host:app1.azurewebsites.net
x-original-host:contoso...
```

app1.azurewebsites.net ✓

app2.azurewebsites.net

Add Backend setting

unaltered to the backend. Multi-tenant services like App S
extension to resolve to the correct endpoint. Change thes

Override with new host name

Yes   No

Host name override

● Pick host name from backend target
○ Override with specific domain name

@DeveloperDaysPL

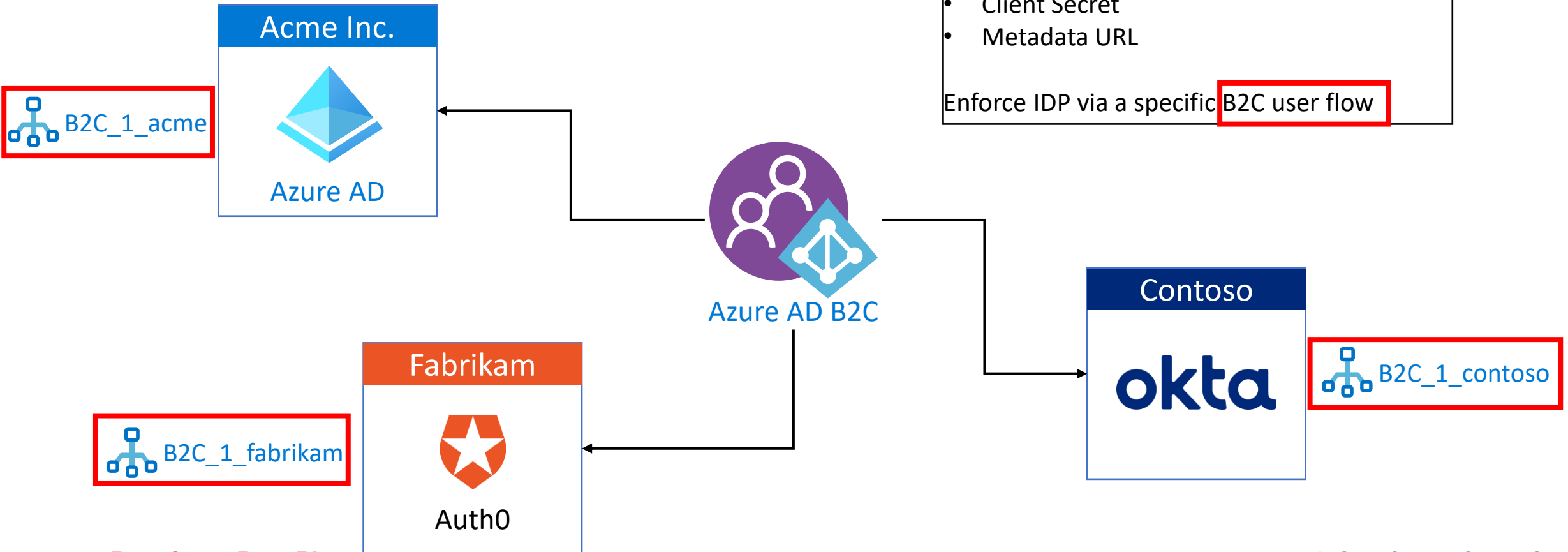net.developerdays.pl

Enterprise-ready security: corporate SSO

We can work with any IDP which supports **OpenID** Connect

- Client ID
- Client Secret
- Metadata URL

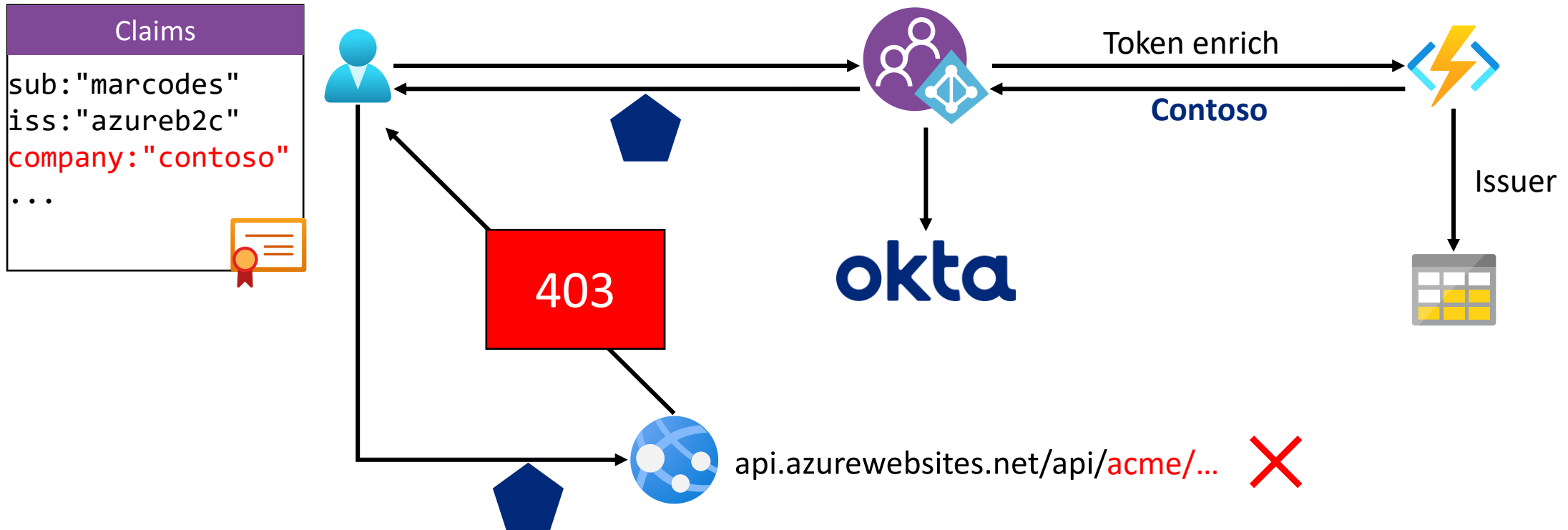Enforce IDP via a specific B2C user flow

B2C_1_acme

Acme Inc.
Azure AD

Fabrikam
Auth0

B2C_1_fabrikam

Azure AD B2C

Contoso
okta

B2C_1_contoso

Demo

Enterprise-ready security

Enterprise-ready security: ring fencing access control

Claims

```
sub:"marcodes"
iss:"azureb2c"
company:"contoso"
...
```

403

Token enrich

Contoso

Issuer

okta

api.azurewebsites.net/api/acme/...

```
internal class ClaimsCompanyContextAccessor
{
    // read CompanyId from the user claims
}
```

```
options.AddPolicy("CompanyMustMatch",
policy ⇒
{
    // check that CompanyId from routing
    // and CompanyId from claims match
});
```

One last question:
What does it take to add a new client?

Recap

- Different data isolation strategies
  - Row Level security
- Subdomain-independent delivery network
- Support for corporate SSO
- Access control in the application
- Creation of a new instance via Graph API

Please rate this session using

.NET DeveloperDays mobile app

(available on Google Play and AppStore)

Thank you! ☺

@crad77
info@marcodesanctis.it

Get the bits at
https://github.com/cradle77/SaaSDemo

Event Sponsors

Strategic Sponsors

Demant

avanade

Gold Sponsors

Relativity®

ProDataConsult

medius

KMD
An NEC Company