



Securing your SaaS offer webhook

Mastering the Marketplace
<https://aka.ms/MasteringTheMarketplace>



Agenda



Basic webhook flow

Implementing webhook security

- .NET app
- Logic app

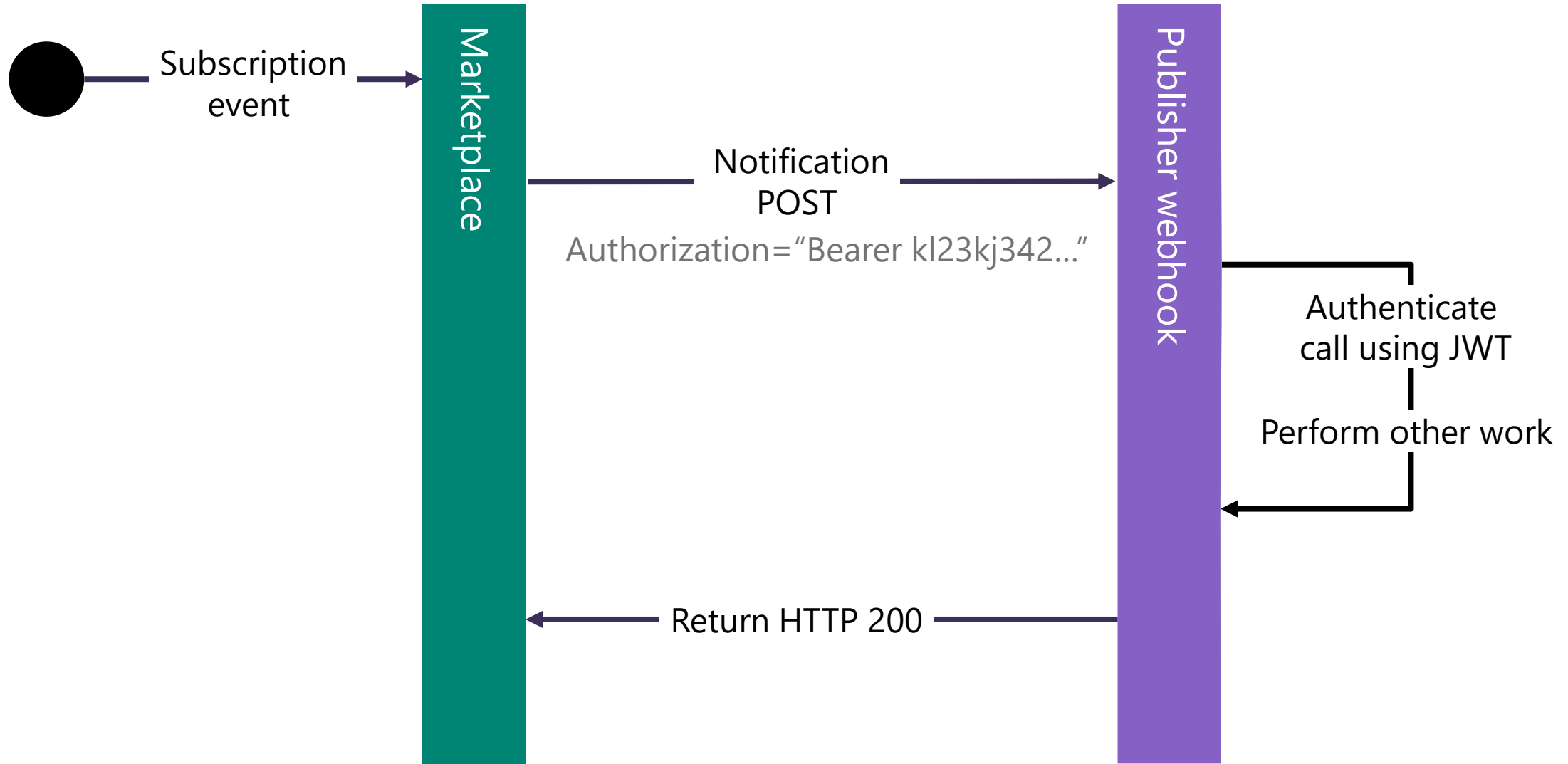
A security anti-pattern



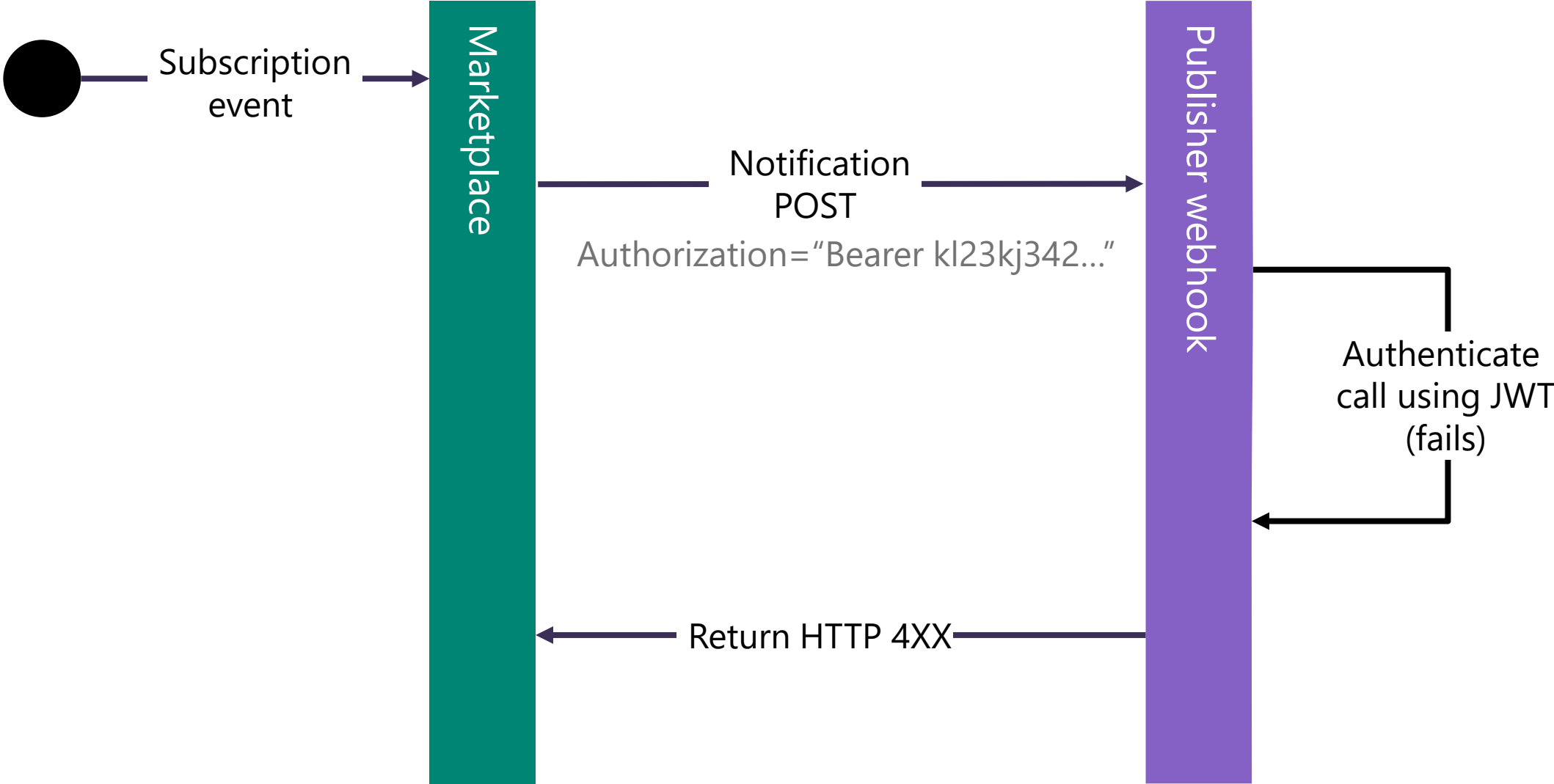
Basic webhook flow

How the marketplace interacts with your webhook and what your webhook should be doing

Webhook POST model



Webhook POST model





Implementing webhook security

How to secure the webhook for your SaaS offers


Calls from the marketplace include a JWT

JWT – JSON Web Token

Use the JWT to validate the call came from the marketplace

Inspect the payload for key information

```
{  
  "appid": "20e940b3-4c77-4b0b-9a53-9e16a1b010a",  
  "aud": "19f1939-4fed-34tb-9e83-9F56a1...",  
  "tid": "64f940b3-3d67-5a0f-0b64-98fd98qwe",  
  "iss": "https://sts.windows.net/64f940b3-3d67-5a0f-0b64-98fd98qwe/",  
  "oid": "ac29bbff-3407-4119-b2d9-866f46d5...",  
  "exp": 1717271173,  
  "ver": "1.0"  
}
```



Key JWT payload information

tid

The Entra tenant ID in the offer's Partner Center technical configuration.

aud

The Entra ID application ID in the offer's Partner Center technical configuration.

appid or **azp**

The resource ID used when you create the authorization token to call SaaS fulfillment APIs.

<https://learn.microsoft.com/partner-center>

Demo

Validating a SaaS webhook
request

Inspecting the marketplace
JWT

Demo

Validating a SaaS webhook
request

Securing a webhook
implemented in .NET

Demo

Validating a SaaS webhook
request

Securing a webhook
implemented with a Logic app

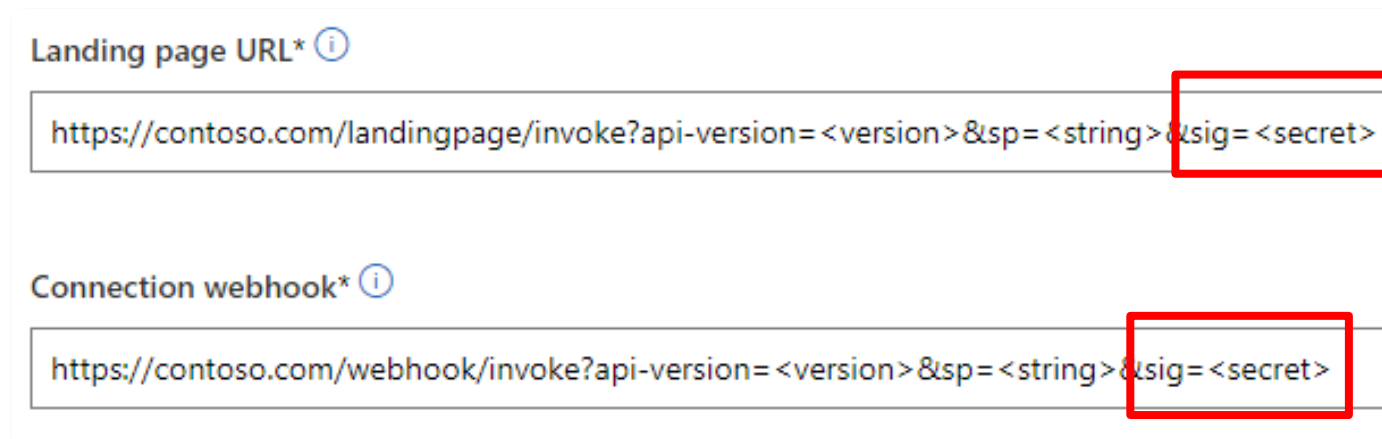


A security anti-pattern

How not to secure your webhook or landing page

Don't do it this way

Technical configuration in Partner Center



Landing page URL* ⓘ

`https://contoso.com/landingpage/invoke?api-version=<version>&sp=<string>&sig=<secret>`

Connection webhook* ⓘ

`https://contoso.com/webhook/invoke?api-version=<version>&sp=<string>&sig=<secret>`

Passing **secrets** in query strings is not allowed

Do not include sensitive information of any kind

This will fail certification

Risks of passing secrets

URL exposure

The key may be compromised via logs.

Accidental sharing

URLs with embedded keys may be shared with unauthorized users.

Security dos and don'ts

Do not add security tokens or other auth details to URLs in Partner Center technical configuration.

Use technology and techniques that accept Authentication headers.

Use the JWT to validate that calls are originating from Microsoft.



Summary



Basic webhook flow

Implementing security for my webhook

- Azure function in .NET
- Logic app

A security anti-pattern