Top Authentication Fails in ASP.NET Core (and How to Avoid Them)

nestenius.se

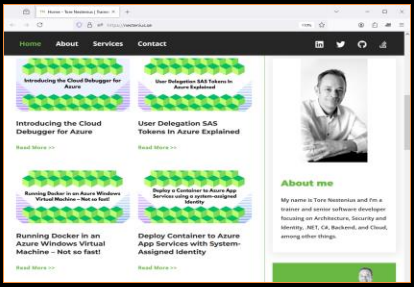
Microsoft Most Valuable Professional

https://nestenius.se

1

About Tore Nestenius

Work https://tn-data.se



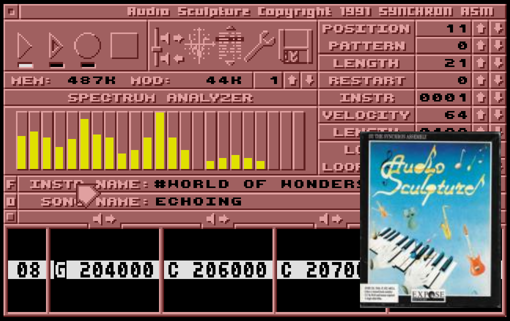
Blog https://nestenius.se

https://meetup.com/net-skane

https://nestenius.se

2

About Tore Nestenius

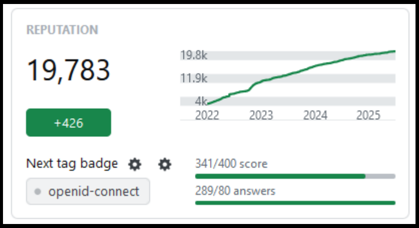


https://nestenius.se

Background

https://nestenius.se

Stack Overflow


REPUTATION

19,783

+426

Next tag badge

openid-connect

341/400 score

289/80 answers

Badges

- IdentityServer4
- OAuth 2.0
- OpenID-Connect
- Authentication
- JWT
- .NET
- C#
- ASP.NET Core

https://nestenius.se

5

What is the goal of this presentation?

- Explore common Authentication Problems
- Learn about various gotchas
- Production challenges

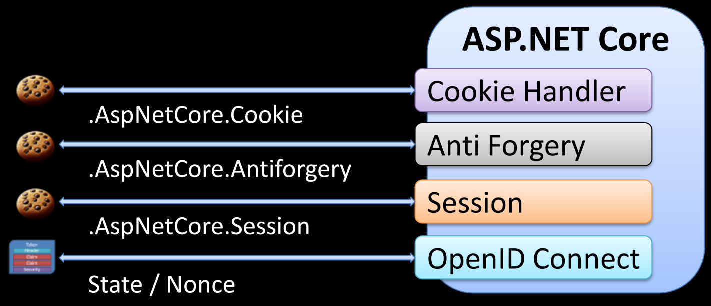
https://nestenius.se

6

Data Protection

Data Protection

ASP.NET Core issues several **sensitive items**, including:

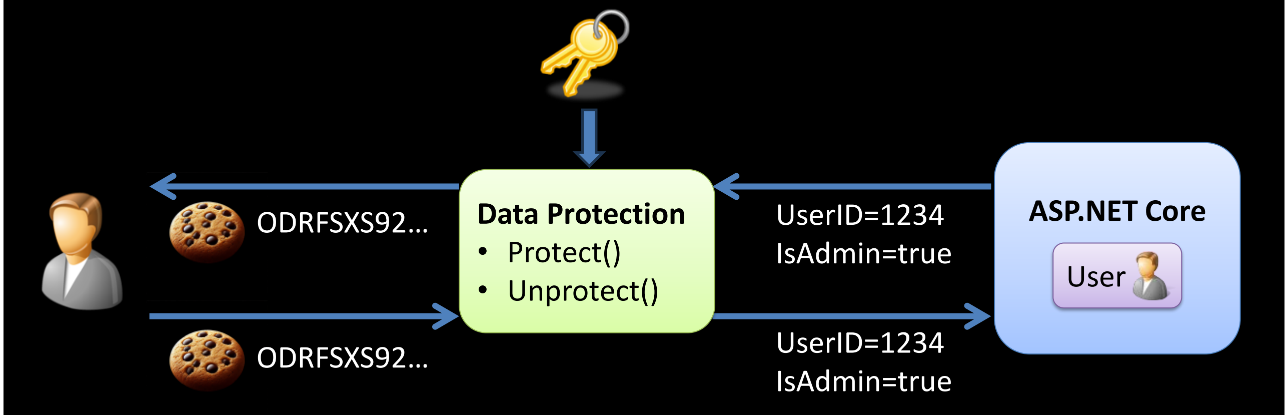


It uses the **Data Protection API** to secure this

How does this work?

Data Protection

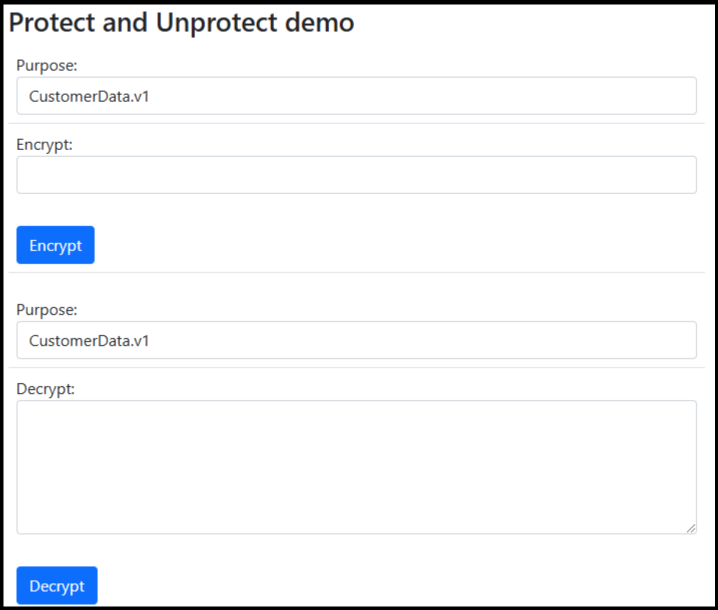
The data is secured using **encryption**



https://nestenius.se

9

Demonstration



Protect and Unprotect demo

Purpose:

CustomerData.v1

Encrypt:

Purpose:

CustomerData.v1

Decrypt:

https://nestenius.se

10

Data Protection in Production

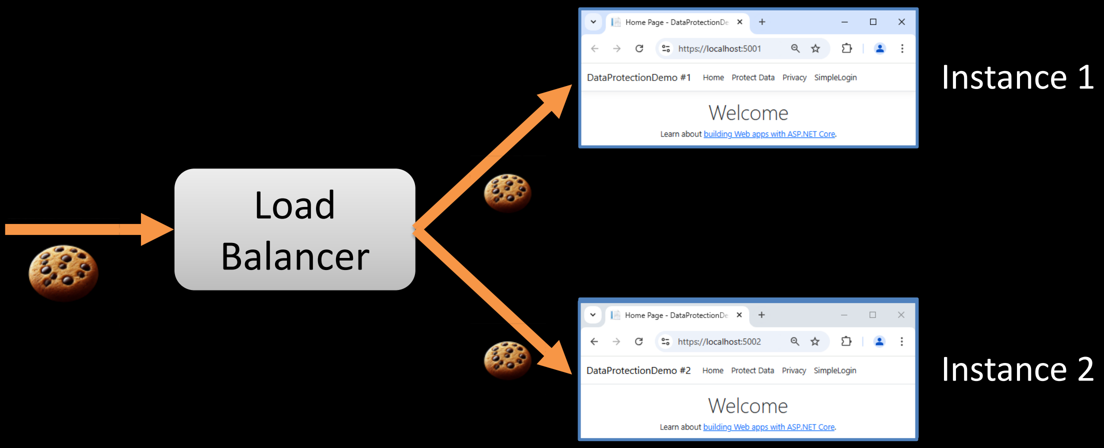
```
Key {} was not found in the key ring. Unprotect operation cannot proceed.

cookie was not authenticated. Failure message: Unprotect ticket failed
```

https://nestenius.se

11

Data Protection

Example Architecture


Load Balancer
Home Page - DataProtectionDe
https://localhost:5001
DataProtectionDemo #1 Home Protect Data Privacy SimpleLogin
Welcome
Learn about building Web apps with ASP.NET Core.
Instance 1
Home Page - DataProtectionDe
https://localhost:5002
DataProtectionDemo #2 Home Protect Data Privacy SimpleLogin
Welcome
Learn about building Web apps with ASP.NET Core.
Instance 2

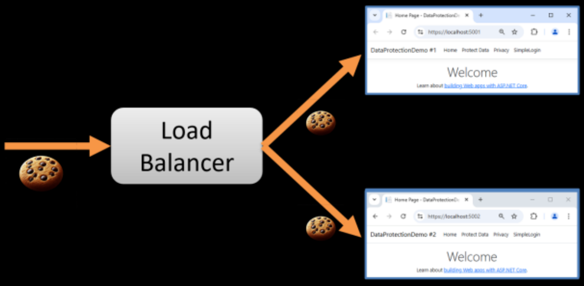
https://nestenius.se

12

Data Protection

What can go wrong here?

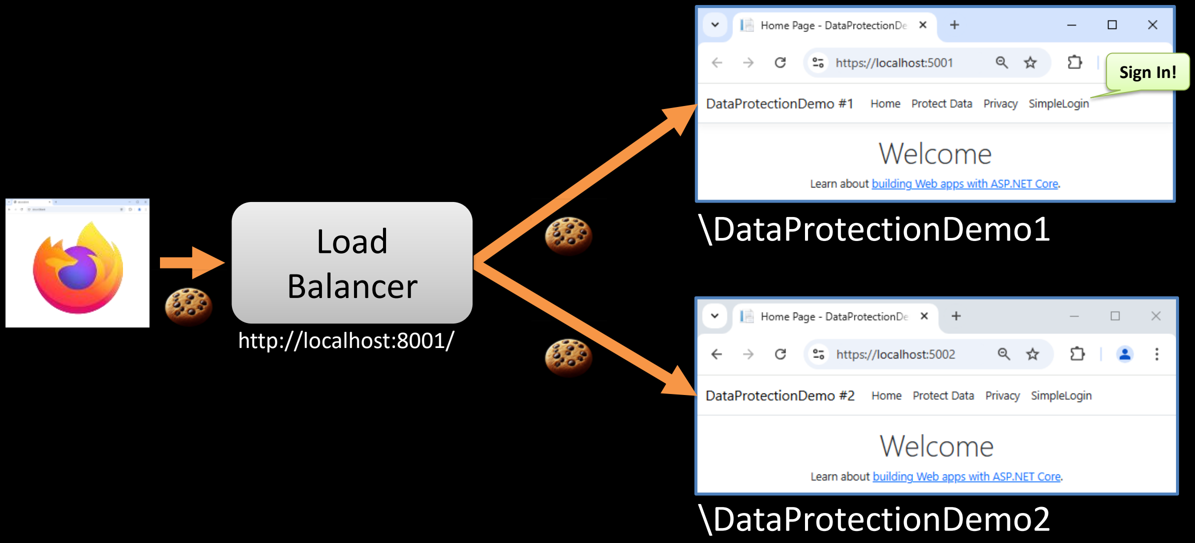
- Users lose their sessions after redeployment
- Cookies aren't recognized across instances
- Key management
- …



What is the problem?

https://nestenius.se

Demonstration – Cookies across service instances

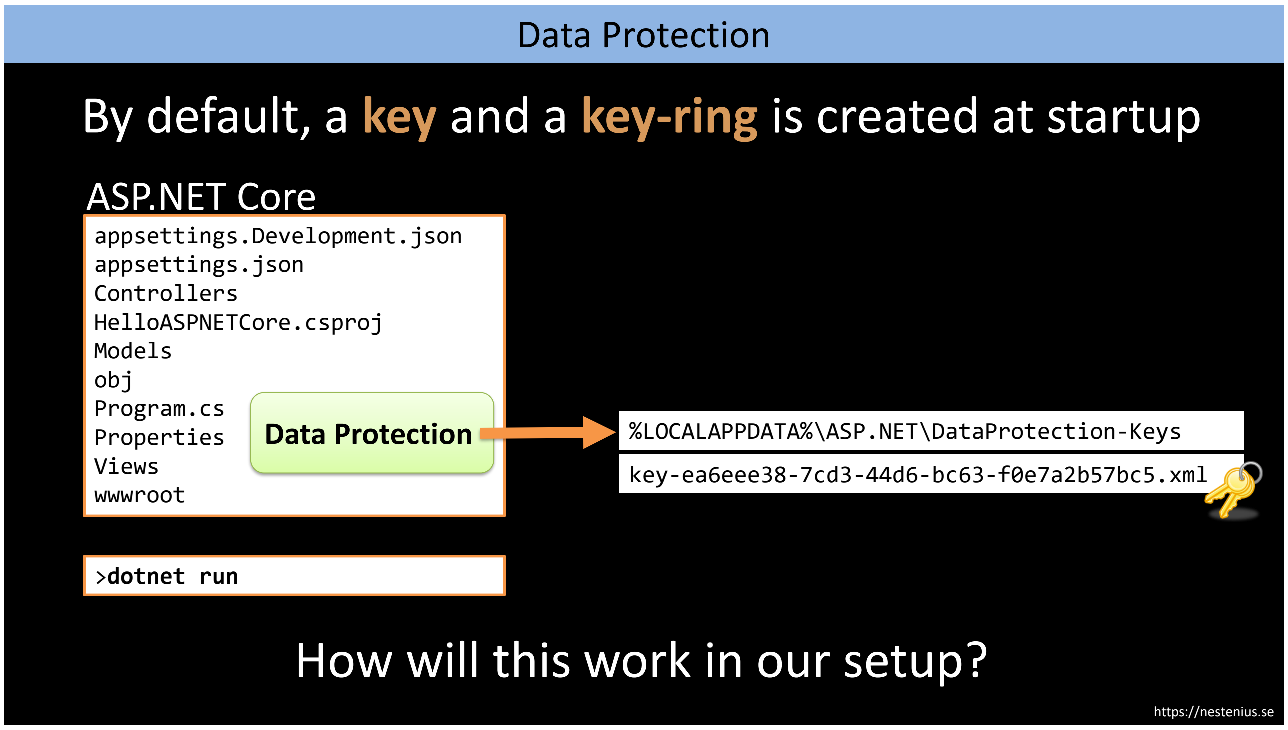

Load Balancer
http://localhost:8001/
Home Page - DataProtectionDe
https://localhost:5001
Sign In!
DataProtectionDemo #1 Home Protect Data Privacy SimpleLogin
Welcome
Learn about building Web apps with ASP.NET Core.
\DataProtectionDemo1
Home Page - DataProtectionDe
https://localhost:5002
DataProtectionDemo #2 Home Protect Data Privacy SimpleLogin
Welcome
Learn about building Web apps with ASP.NET Core.
\DataProtectionDemo2

https://nestenius.se

Data Protection at Startup

https://nestenius.se

15



Data Protection

By default, a **key** and a **key-ring** is created at startup

ASP.NET Core

```
appsettings.Development.json
appsettings.json
Controllers
HelloASPNETCore.csproj
Models
obj
Program.cs
Properties
Views
wwwroot
```

```
%LOCALAPPDATA%\ASP.NET\DataProtection-Keys
key-ea6eee38-7cd3-44d6-bc63-f0e7a2b57bc5.xml
```

```
>dotnet run
```

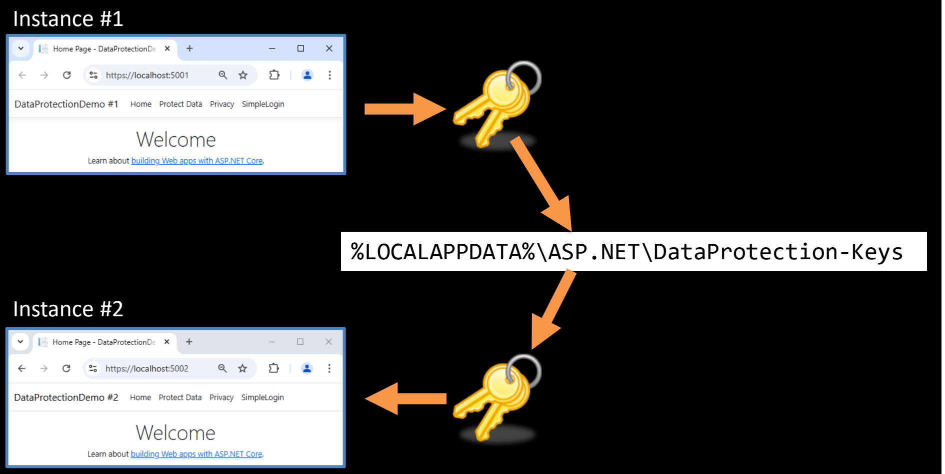
How will this work in our setup?

https://nestenius.se

16

Data Protection

The following happens in our example:


Instance #1
Home Page - DataProtectionDe
https://localhost:5001
DataProtectionDemo #1 Home Protect Data Privacy SimpleLogin
Welcome
Learn about building Web apps with ASP.NET Core.
%LOCALAPPDATA%\ASP.NET\DataProtection-Keys
Instance #2
Home Page - DataProtectionDe
https://localhost:5002
DataProtectionDemo #2 Home Protect Data Privacy SimpleLogin
Welcome
Learn about building Web apps with ASP.NET Core.

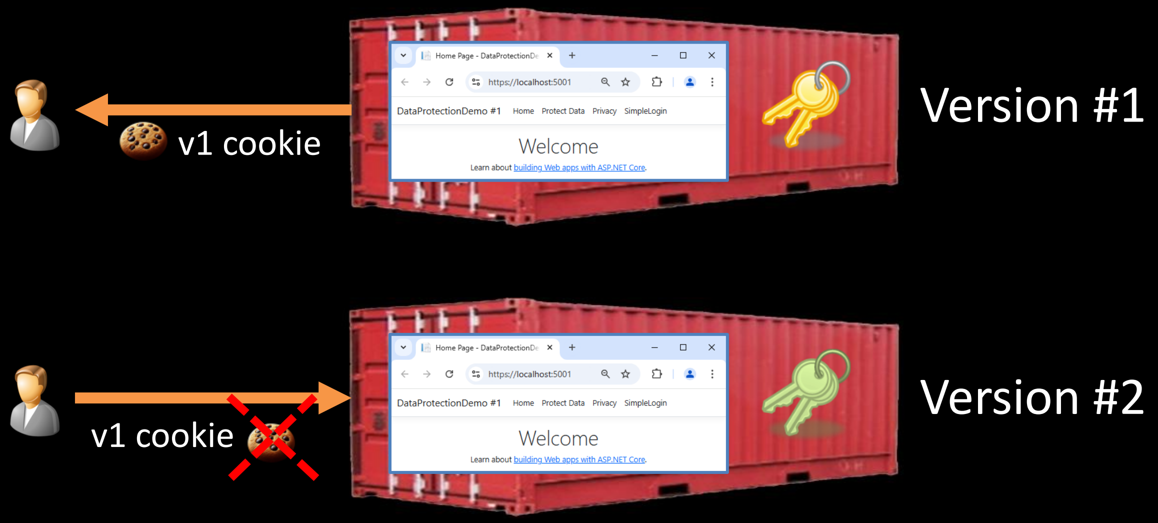
What can go wrong here?

https://nestenius.se

17

Data Protection

Cookies will be rejected if the key changes after redeploy

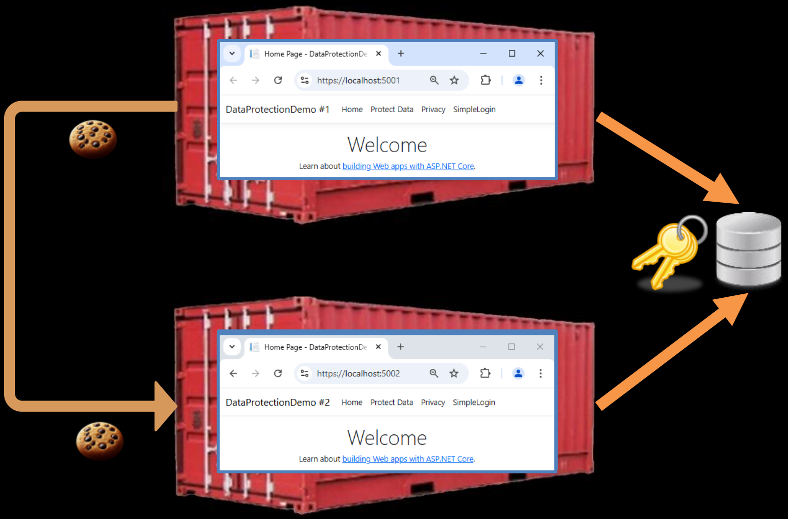

v1 cookie
Home Page - DataProtectionDe
https://localhost:5001
DataProtectionDemo #1 Home Protect Data Privacy SimpleLogin
Welcome
Learn about building Web apps with ASP.NET Core.
Version #1
v1 cookie
Home Page - DataProtectionDe
https://localhost:5001
DataProtectionDemo #1 Home Protect Data Privacy SimpleLogin
Welcome
Learn about building Web apps with ASP.NET Core.
Version #2

https://nestenius.se

18

Data Protection

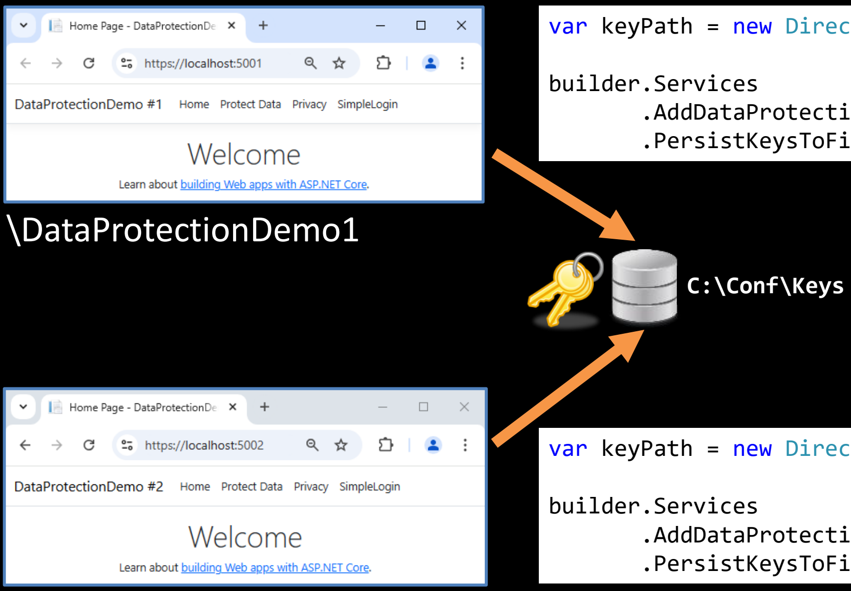
The **key-ring** needs to be persisted in a shared storage


Home Page - DataProtectionDe
https://localhost:5001
DataProtectionDemo #1 Home Protect Data Privacy SimpleLogin
Welcome
Learn about building Web apps with ASP.NET Core.
Home Page - DataProtectionDe
https://localhost:5002
DataProtectionDemo #2 Home Protect Data Privacy SimpleLogin
Welcome
Learn about building Web apps with ASP.NET Core.

- Disk
- Database
- Azure Key Vault
- Blob Storage
- MySQL
- Redis
- …

https://nestenius.se

Demonstration – Persist Keys To File System


Home Page - DataProtectionDe
https://localhost:5001
DataProtectionDemo #1 Home Protect Data Privacy SimpleLogin
Welcome
Learn about building Web apps with ASP.NET Core.
Home Page - DataProtectionDe
https://localhost:5002
DataProtectionDemo #2 Home Protect Data Privacy SimpleLogin
Welcome
Learn about building Web apps with ASP.NET Core.
C:\Conf\Keys

\DataProtectionDemo1

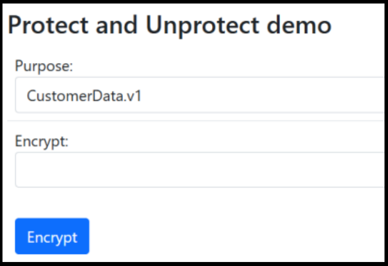
```
var keyPath = new DirectoryInfo(@"C:\Conf\Keys");

builder.Services
       .AddDataProtection()
       .PersistKeysToFileSystem(keyPath);
```

\DataProtectionDemo2

```
var keyPath = new DirectoryInfo(@"C:\Conf\Keys");

builder.Services
       .AddDataProtection()
       .PersistKeysToFileSystem(keyPath);
```

https://nestenius.se

Data Protection Purpose


Protect and Unprotect demo

Purpose:

CustomerData.v1

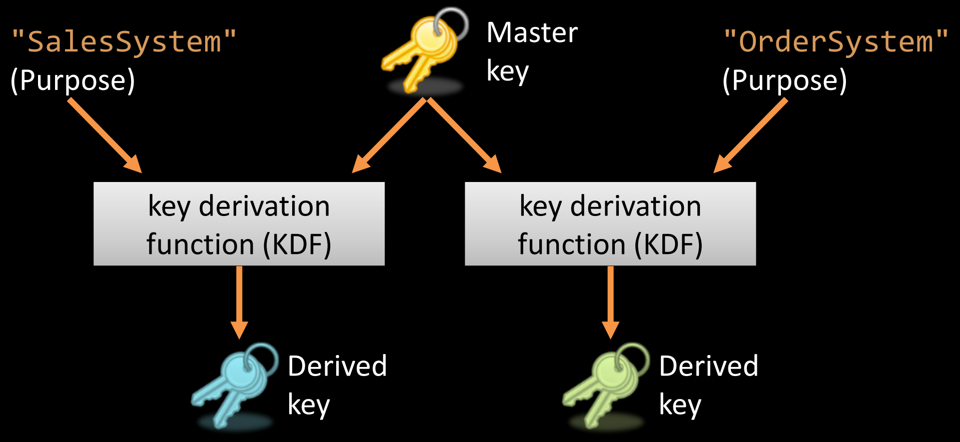
Encrypt:

https://nestenius.se

21

Data Protection Purpose

The **purpose** is used to create isolation



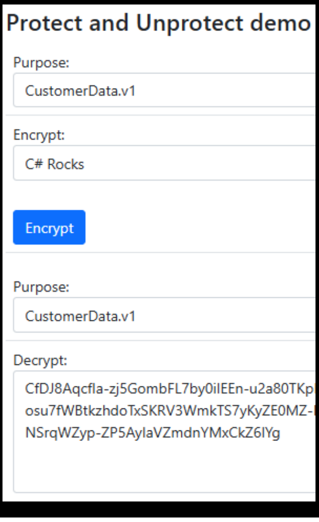
https://nestenius.se

22

Demonstration - Purpose

Why does this not work?

Instance #1



Protect and Unprotect demo

Purpose:

CustomerData.v1

Encrypt:

C# Rocks

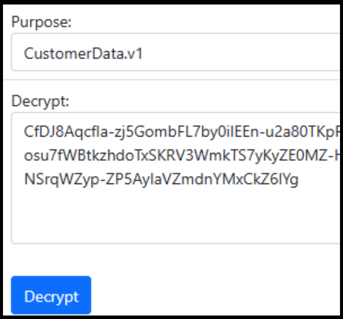
Purpose:

CustomerData.v1

Decrypt:

CfDJ8Aqcfla-zj5GombFL7by0ilEEn-u2a80TKp
osu7fWBtkzhdoTxSKRV3WmkTS7yKyZE0MZ-
NSrqWZyp-ZP5AylaVZmdnYMxCkZ6lYg

Instance #2



Purpose:

CustomerData.v1

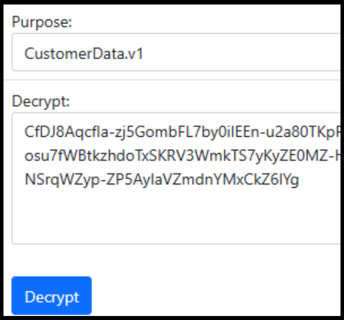
Decrypt:

CfDJ8Aqcfla-zj5GombFL7by0ilEEn-u2a80TKpF
osu7fWBtkzhdoTxSKRV3WmkTS7yKyZE0MZ-H
NSrqWZyp-ZP5AylaVZmdnYMxCkZ6lYg

https://nestenius.se

Data Protection Purpose

We actually have two purposes!



Purpose:

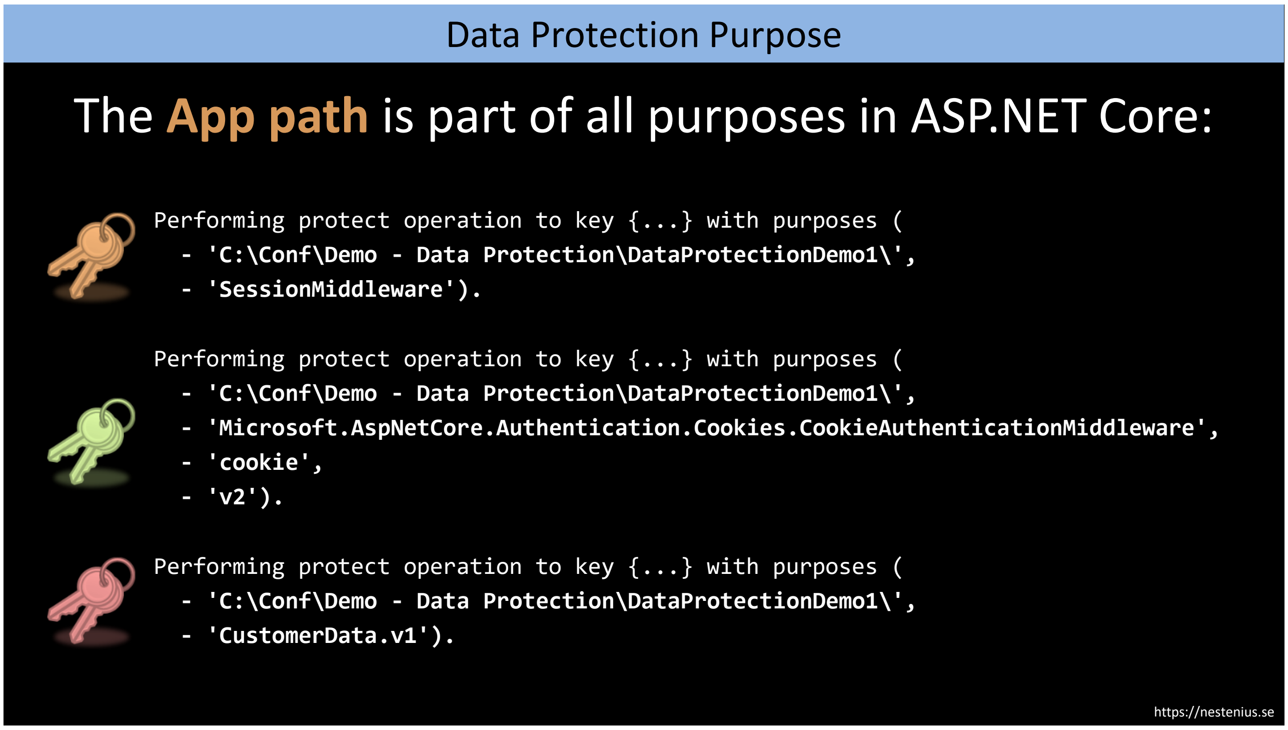
CustomerData.v1

Decrypt:

CfDJ8Aqcfla-zj5GombFL7by0ilEEn-u2a80TKpF
osu7fWBtkzhdoTxSKRV3WmkTS7yKyZE0MZ-H
NSrqWZyp-ZP5AylaVZmdnYMxCkZ6lYg

```
Performing unprotect operation to key {bc7e21f3-69e3-45ce-bb5b-e9007bac85ed}
with purposes ('C:\Conf\Demo - Data Protection\DataProtectionDemo1\',
                'CustomerData.v1').
```

https://nestenius.se



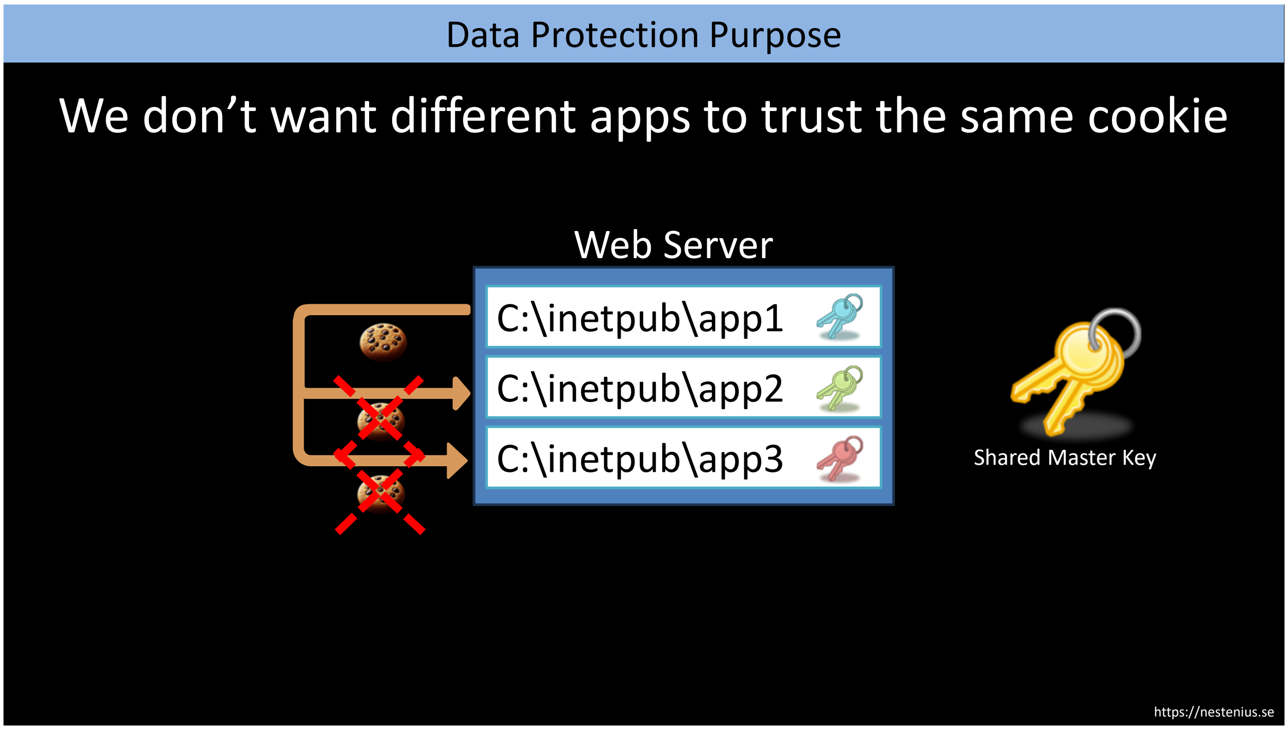
Data Protection Purpose

The **App path** is part of all purposes in ASP.NET Core:

```
Performing protect operation to key {...} with purposes (
  - 'C:\Conf\Demo - Data Protection\DataProtectionDemo1\',
  - 'SessionMiddleware').

Performing protect operation to key {...} with purposes (
  - 'C:\Conf\Demo - Data Protection\DataProtectionDemo1\',
  - 'Microsoft.AspNetCore.Authentication.Cookies.CookieAuthenticationMiddleware',
  - 'cookie',
  - 'v2').

Performing protect operation to key {...} with purposes (
  - 'C:\Conf\Demo - Data Protection\DataProtectionDemo1\',
  - 'CustomerData.v1').
```

https://nestenius.se

25



Data Protection Purpose

We don’t want different apps to trust the same cookie

https://nestenius.se

26

Demonstration – Set Application Name

We can replace the path with an application name

```
var keyPath = new DirectoryInfo(@"C:\Conf\Keys");

builder.Services.AddDataProtection()
                .PersistKeysToFileSystem(keyPath)
                .SetApplicationName("MyApplication");
```

https://nestenius.se

27

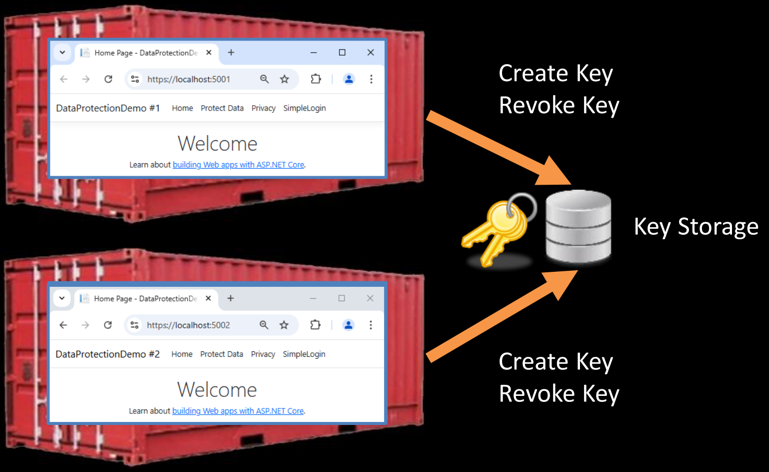
Key Management Problems

https://nestenius.se

28

Key Management Problems

By default, both services wants to manage the keys


Home Page - DataProtectionDe
https://localhost:5001
DataProtectionDemo #1 Home Protect Data Privacy SimpleLogin
Welcome
Learn about building Web apps with ASP.NET Core.
Create Key
Revoke Key
Key Storage
Home Page - DataProtectionDe
https://localhost:5002
DataProtectionDemo #2 Home Protect Data Privacy SimpleLogin
Welcome
Learn about building Web apps with ASP.NET Core.
Create Key
Revoke Key

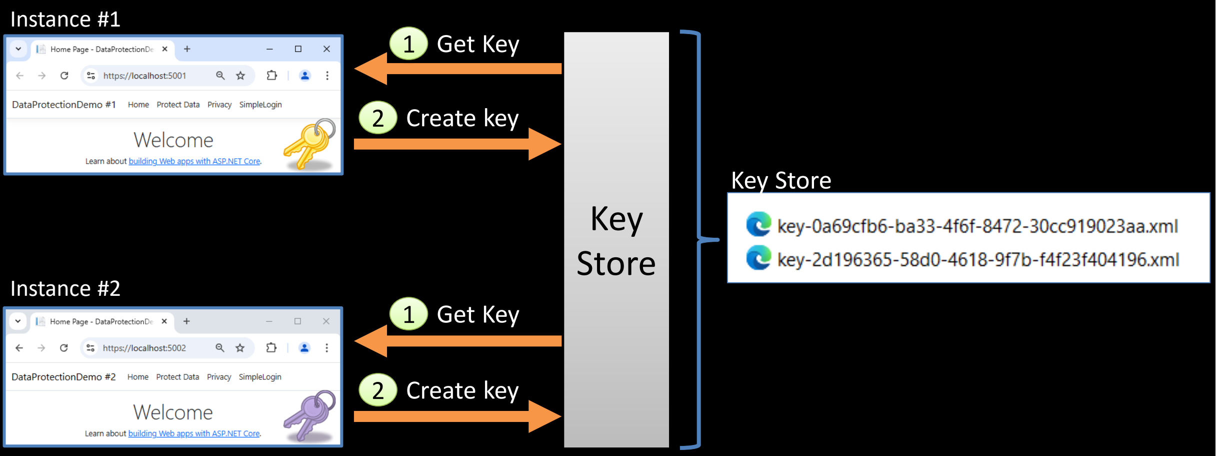
What can go wrong here?

https://nestenius.se

29

Data Protection

What if both instances try to create a new key?


Instance #1
Home Page - DataProtectionDe
https://localhost:5001
DataProtectionDemo #1 Home Protect Data Privacy SimpleLogin
Welcome
Learn about building Web apps with ASP.NET Core.
1 Get Key
2 Create key
Key Store
Key Store
key-0a69cfb6-ba33-4f6f-8472-30cc919023aa.xml
key-2d196365-58d0-4618-9f7b-f4f23f404196.xml
Instance #2
Home Page - DataProtectionDe
https://localhost:5002
DataProtectionDemo #2 Home Protect Data Privacy SimpleLogin
Welcome
Learn about building Web apps with ASP.NET Core.
1 Get Key
2 Create key

Why is this a problem?

https://nestenius.se

30

Data Protection

We can get a race condition!

Instance #1

```
2025-02-03T16:28:44 Repository contains no viable default key.
                    Caller should generate a key with immediate activation.
2025-02-03T16:28:44 Policy resolution states that a new key should be added to the key ring.
2025-02-03T16:28:44 Creating key {0a69cfb6-ba33-4f6f-8472-30cc919023aa} with
                    creation date 2025-02-03 15:28:44Z, activation date 2025-02-03 15:28:44Z,
                    and expiration date 2025-05-04 15:28:44Z.
```

Instance #2

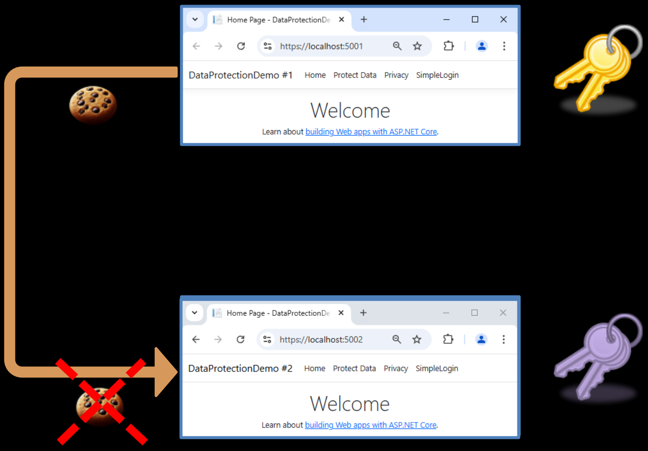
```
2025-02-03T16:28:44 Repository contains no viable default key.
                    Caller should generate a key with immediate activation.
2025-02-03T16:28:44 Policy resolution states that a new key should be added to the key ring.
2025-02-03T16:28:44 Creating key {2d196365-58d0-4618-9f7b-f4f23f404196} with
                    creation date 2025-02-03 15:28:44Z, activation date 2025-02-03 15:28:44Z,
                    and expiration date 2025-05-04 15:28:44Z.
```

Why is this a problem in production?

https://nestenius.se

Data Protection

Cookies will be rejected across service instances


Home Page - DataProtectionDe
https://localhost:5001
DataProtectionDemo #1 Home Protect Data Privacy SimpleLogin
Welcome
Learn about building Web apps with ASP.NET Core.
Home Page - DataProtectionDe
https://localhost:5002
DataProtectionDemo #2 Home Protect Data Privacy SimpleLogin
Welcome
Learn about building Web apps with ASP.NET Core.

How can we solve this?

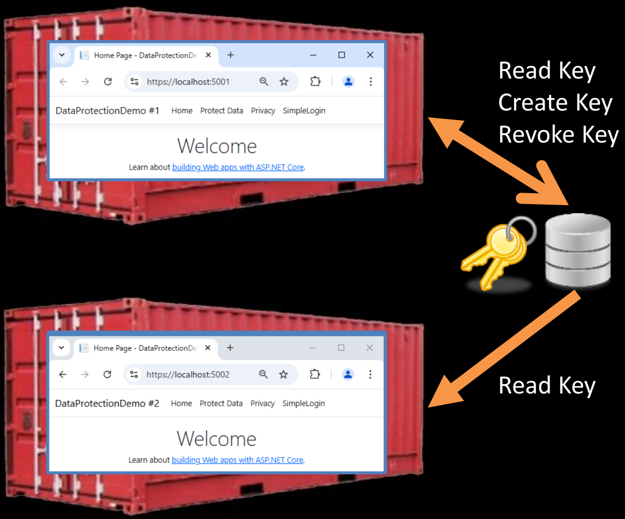
https://nestenius.se

Key Management Problems

You can control which instance can create keys

```
// Primary
builder.Services.AddDataProtection()
   .SetApplicationName("MyApplication");
```

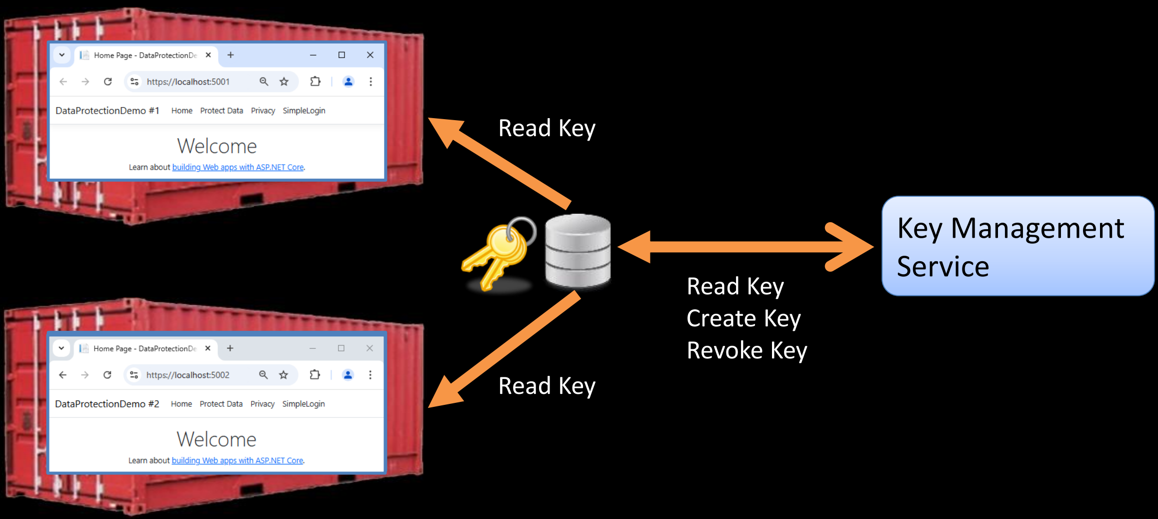
```
// Secondary
builder.Services.AddDataProtection()
   .SetApplicationName("MyApplication")
   .DisableAutomaticKeyGeneration();
```



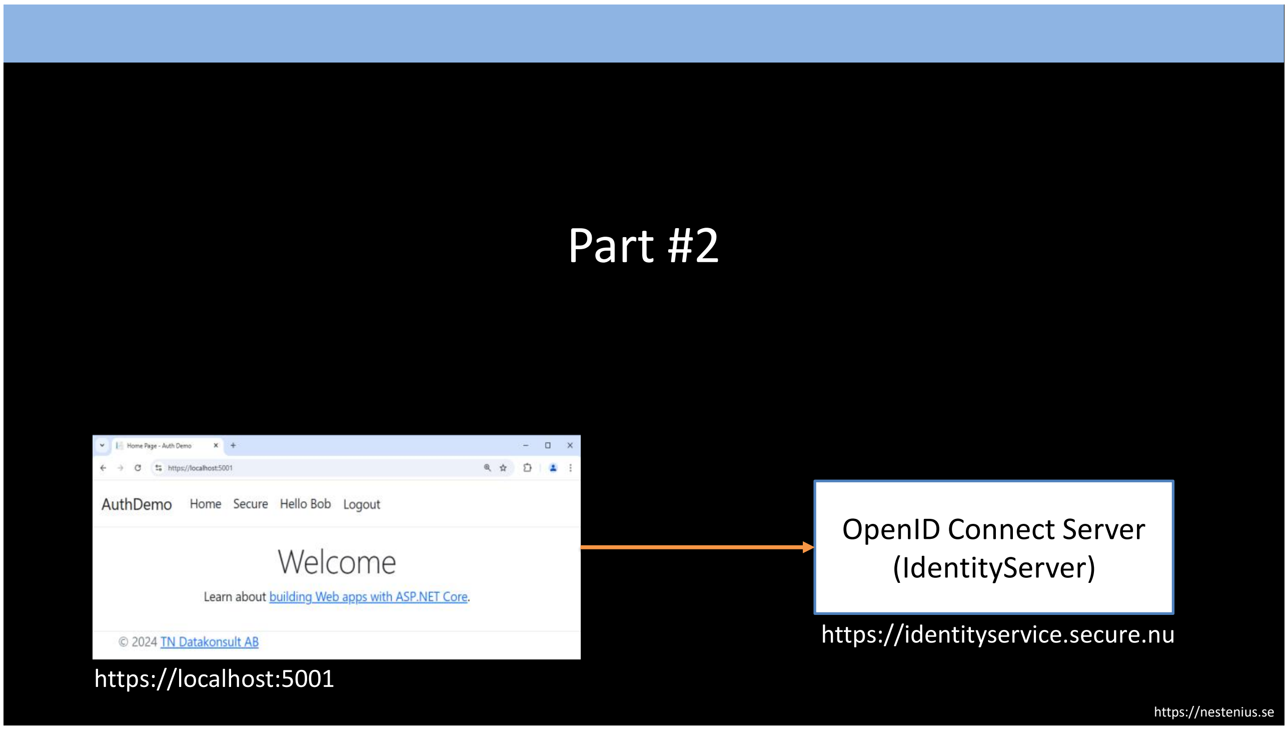
https://nestenius.se

Key Management Problems

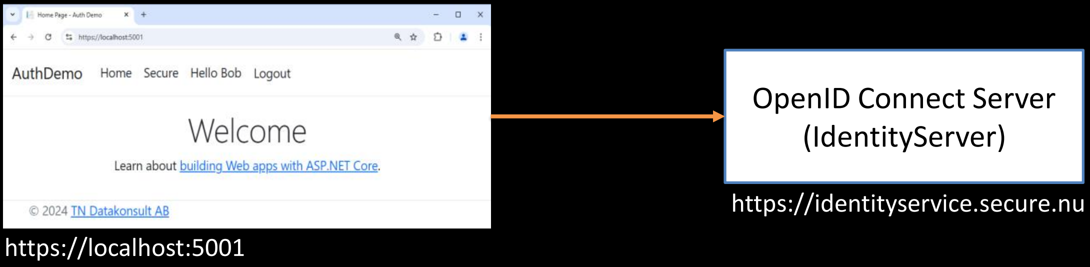
Or, you can use a separate service to manage keys



https://nestenius.se

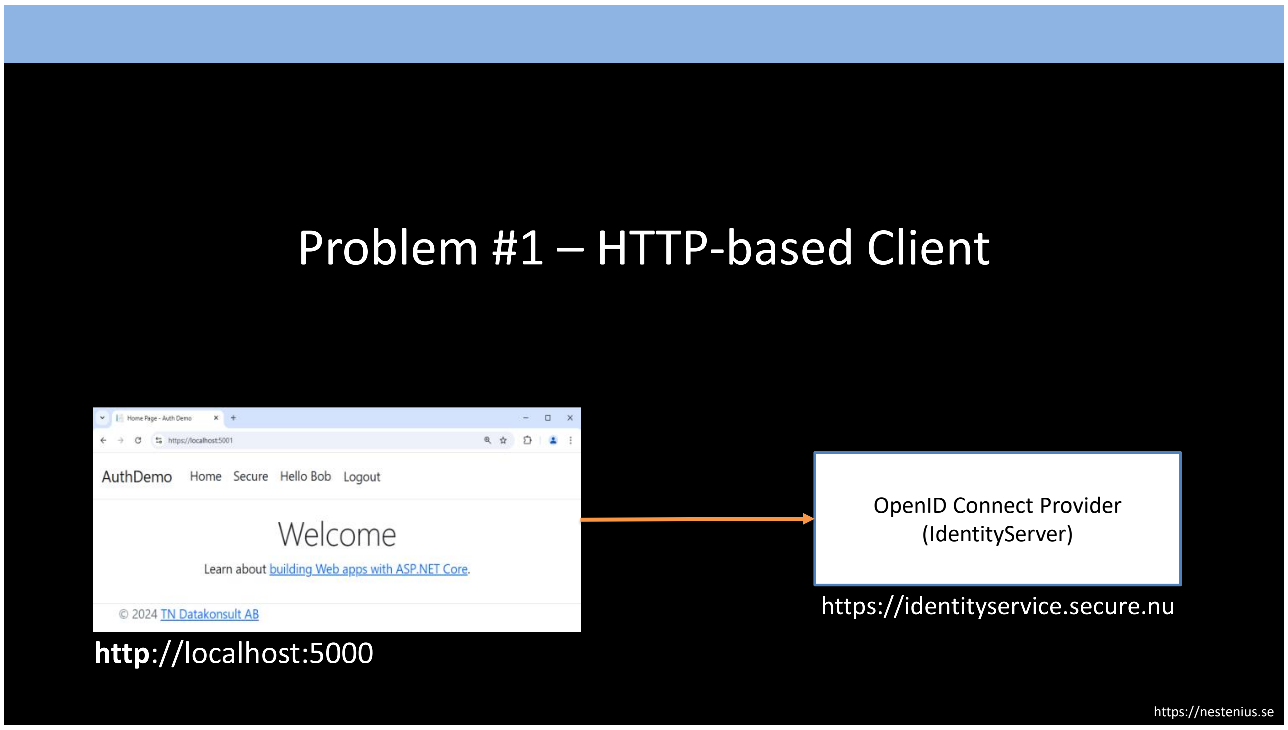


Part #2

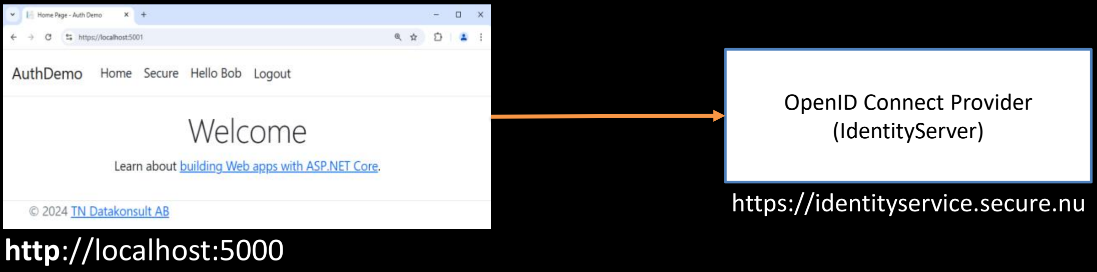


https://nestenius.se

35



Problem #1 – HTTP-based Client

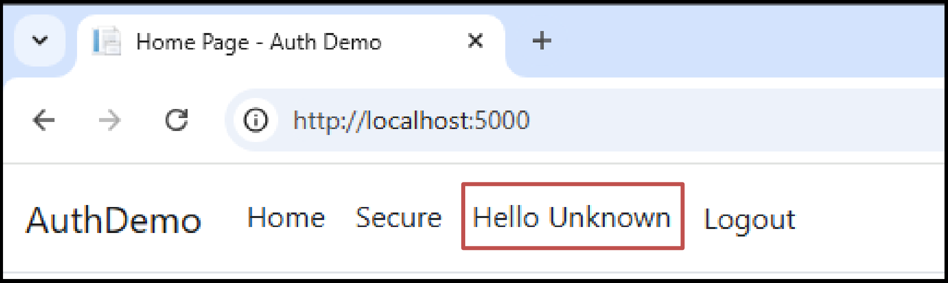

Home Page - Auth Demo
https://localhost:5001
AuthDemo
Home
Secure
Hello Bob
Logout
Welcome
Learn about building Web apps with ASP.NET Core.
© 2024 TN Datakonsult AB
http://localhost:5000
OpenID Connect Provider (IdentityServer)
https://identityservice.secure.nu

https://nestenius.se

36

Problem #1 – HTTP-based Client

OIDC Authenticating over **HTTP** Works great!



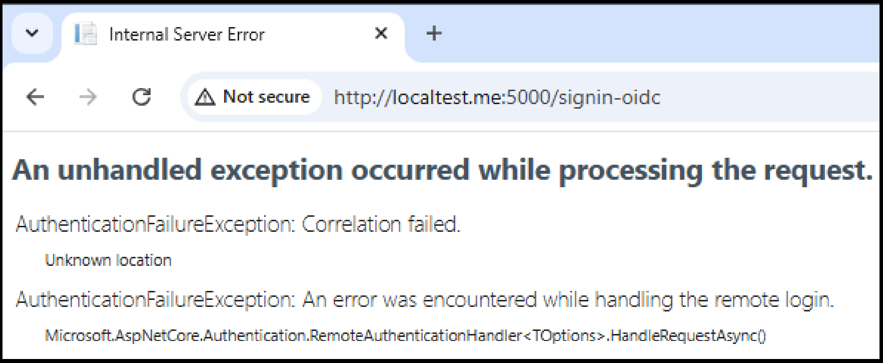
However, we have a problem!

https://nestenius.se

37

Problem #1 – HTTP-based Client

Authenticating over a **non-localhost** domain fails!



An unhandled exception occurred while processing the request.

AuthenticationFailureException: Correlation failed.

Unknown location

AuthenticationFailureException: An error was encountered while handling the remote login.

Microsoft.AspNetCore.Authentication.RemoteAuthenticationHandler<TOptions>.HandleRequestAsync()

Why does it work over **localhost**?

https://nestenius.se

38

Problem #1 – HTTP-based Client

These are considered **Potentially Trustworthy**

- `http://127.0.0.1`
- `http://localhost`
- `http://*.localhost`
- `file://`

https://nestenius.se

Demonstration

```
<h1>Is this context secure?</h1>
<p id="secure-status">Checking...</p>

<script>
    const isSecure = window.isSecureContext

    document.getElementById('secure-status').textContent =
        isSecure ? "Yes, this is a secure context." :
                   "No, this is not a secure context.";
</script>
```

https://nestenius.se

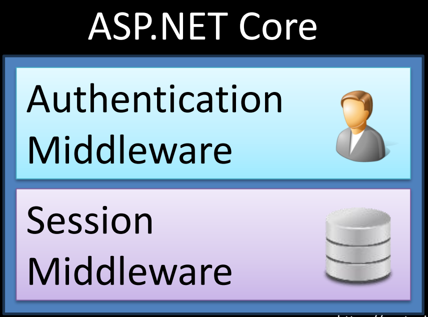
Problem #2 – Cookie Confusion

Cookie Confusion

What is the difference?

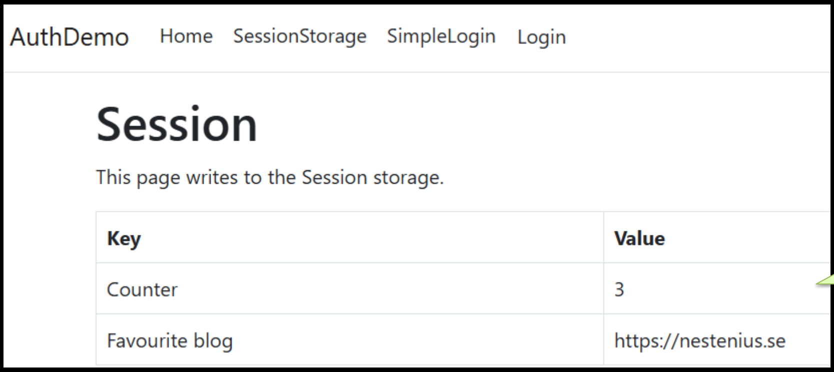
Name	Value	Domain	Path	Expires / Max-A...	Size
.AspNetCore.cookie	CfDJ8GiF8Bbiy1RIrW0...	localhost	/	Session	2968
.AspNetCore.Session	CfDJ8GiF8Bbiy1RIrW0...	localhost	/	Session	207

- AspNetCore.cookie
  - User authentication session (User login)
- AspNetCore.Session
  - Temporary session data



Demonstration – Cookie Confusion

Using the Session Service

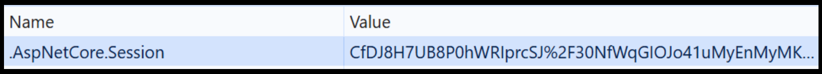


Session

This page writes to the Session storage.

Key	Value
Counter	3
Favourite blog	https://nestenius.se

Reload!



Name	Value
.AspNetCore.Session	CfDJ8H7UB8P0hWRIprcSJ%2F30NfWqGIOJo41uMyEnMyMK...

https://nestenius.se

43

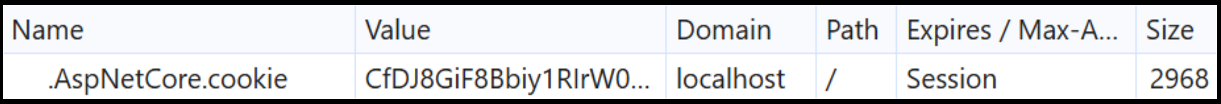
Cookies Ingredients

https://nestenius.se

44

Cookies Ingredients

What is inside the authentication cookie?



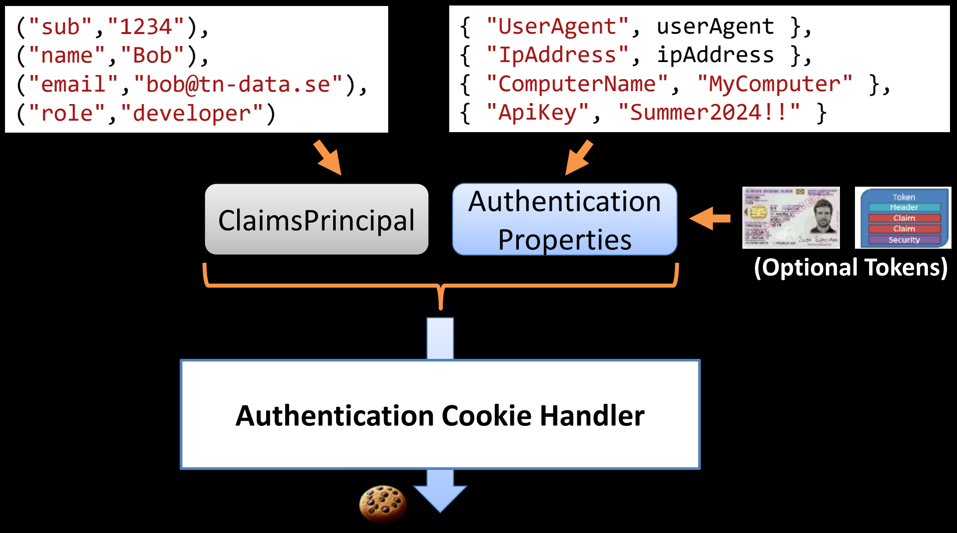
Name	Value	Domain	Path	Expires / Max-A...	Size
.AspNetCore.cookie	CfDJ8GiF8Bbiy1RIrW0...	localhost	/	Session	2968

Let's find out!

https://nestenius.se

45

Cookies Ingredients



```
("sub","1234"),
("name","Bob"),
("email","bob@tn-data.se"),
("role","developer")
```

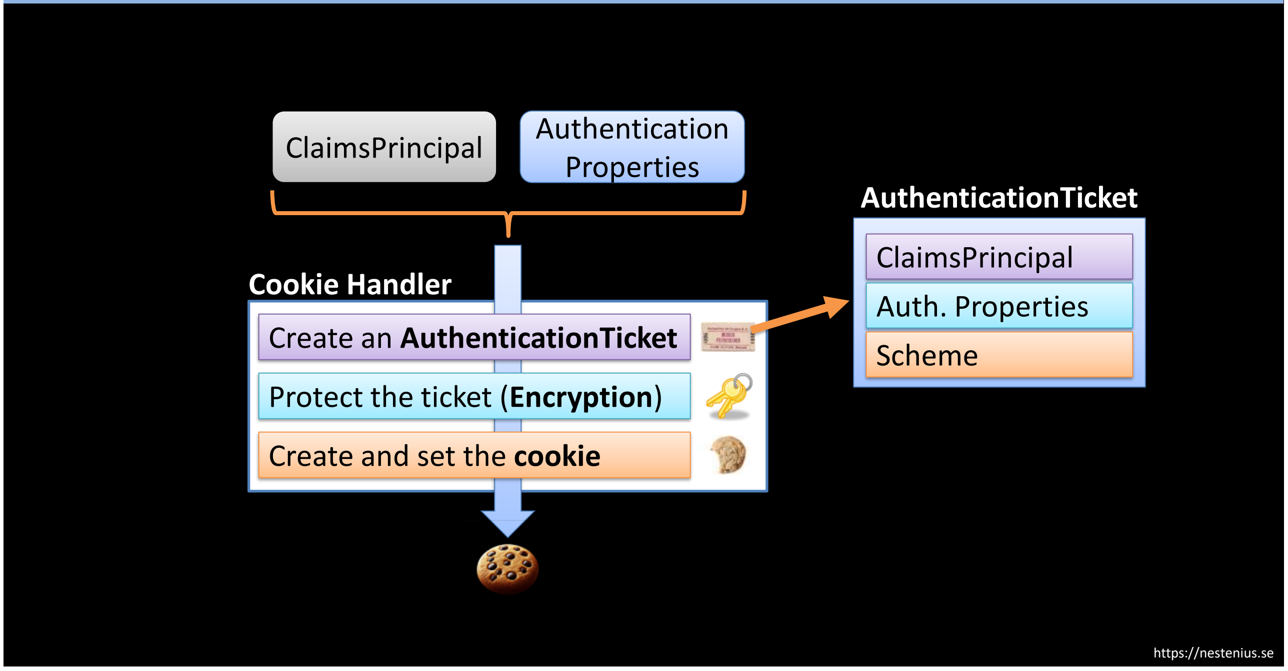
```
{ "UserAgent", userAgent },
{ "IpAddress", ipAddress },
{ "ComputerName", "MyComputer" },
{ "ApiKey", "Summer2024!!" }
```

What happens inside the Cookie Handler?

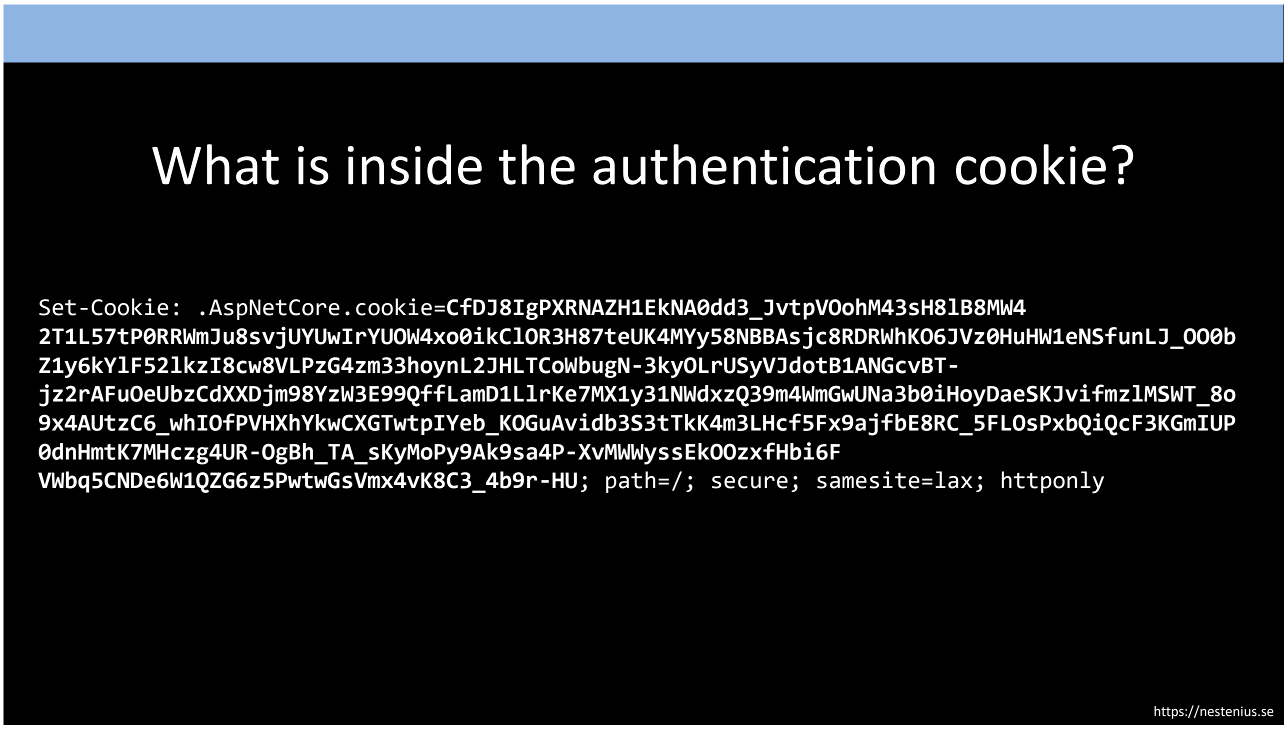
https://nestenius.se

46

Cookies Ingredients


ClaimsPrincipal
Authentication Properties
Cookie Handler
Create an **AuthenticationTicket**
Protect the ticket (**Encryption**)
Create and set the **cookie**
AuthenticationTicket
ClaimsPrincipal
Auth. Properties
Scheme
https://nestenius.se

47

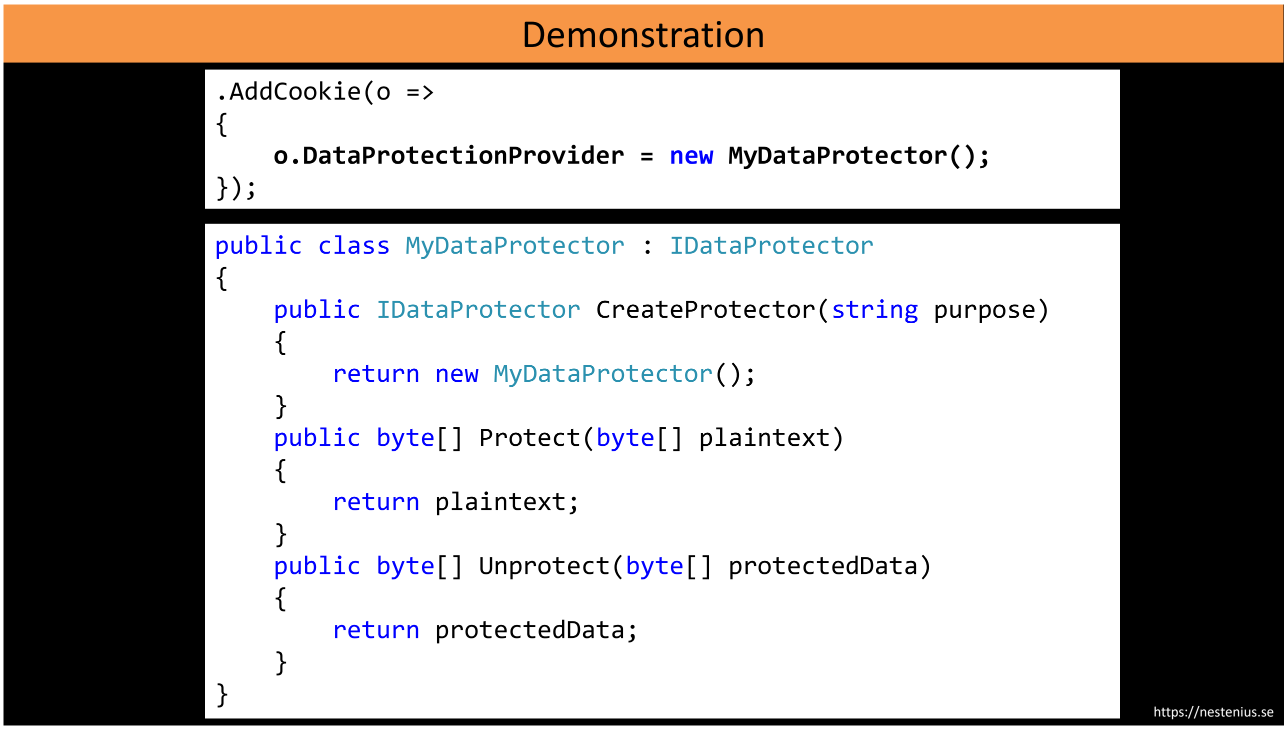


What is inside the authentication cookie?

```
Set-Cookie: .AspNetCore.cookie=CfDJ8IgPXRNAZH1EkNA0dd3_JvtpVOohM43sH8lB8MW4
2T1L57tP0RRWmJu8svjUYUwIrYUOW4xo0ikClOR3H87teUK4MYy58NBBAsjc8RDRWhKO6JVz0HuHW1eNSfunLJ_OO0b
Z1y6kYlF52lkzI8cw8VLPzG4zm33hoynL2JHLTCoWbugN-3kyOLrUSyVJdotB1ANGcvBT-
jz2rAFuOeUbzCdXXDjm98YzW3E99QffLamD1LlrKe7MX1y31NWdxzQ39m4WmGwUNa3b0iHoyDaeSKJvifmzlMSWT_8o
9x4AUtzC6_whIOfPVHXhYkwCXGTwtpIYeb_KOGuAvidb3S3tTkK4m3LHcf5Fx9ajfbE8RC_5FLOsPxbQiQcF3KGmIUP
0dnHmtK7MHczg4UR-OgBh_TA_sKyMoPy9Ak9sa4P-XvMWWyssEkOOzxfHbi6F
VWbq5CNDe6W1QZG6z5PwtwGsVmx4vK8C3_4b9r-HU; path=/; secure; samesite=lax; httponly
```

https://nestenius.se

48



Demonstration

```
.AddCookie(o =>
{
    o.DataProtectionProvider = new MyDataProtector();
});
```

```
public class MyDataProtector : IDataProtector
{
    public IDataProtector CreateProtector(string purpose)
    {
        return new MyDataProtector();
    }
    public byte[] Protect(byte[] plaintext)
    {
        return plaintext;
    }
    public byte[] Unprotect(byte[] protectedData)
    {
        return protectedData;
    }
}
```

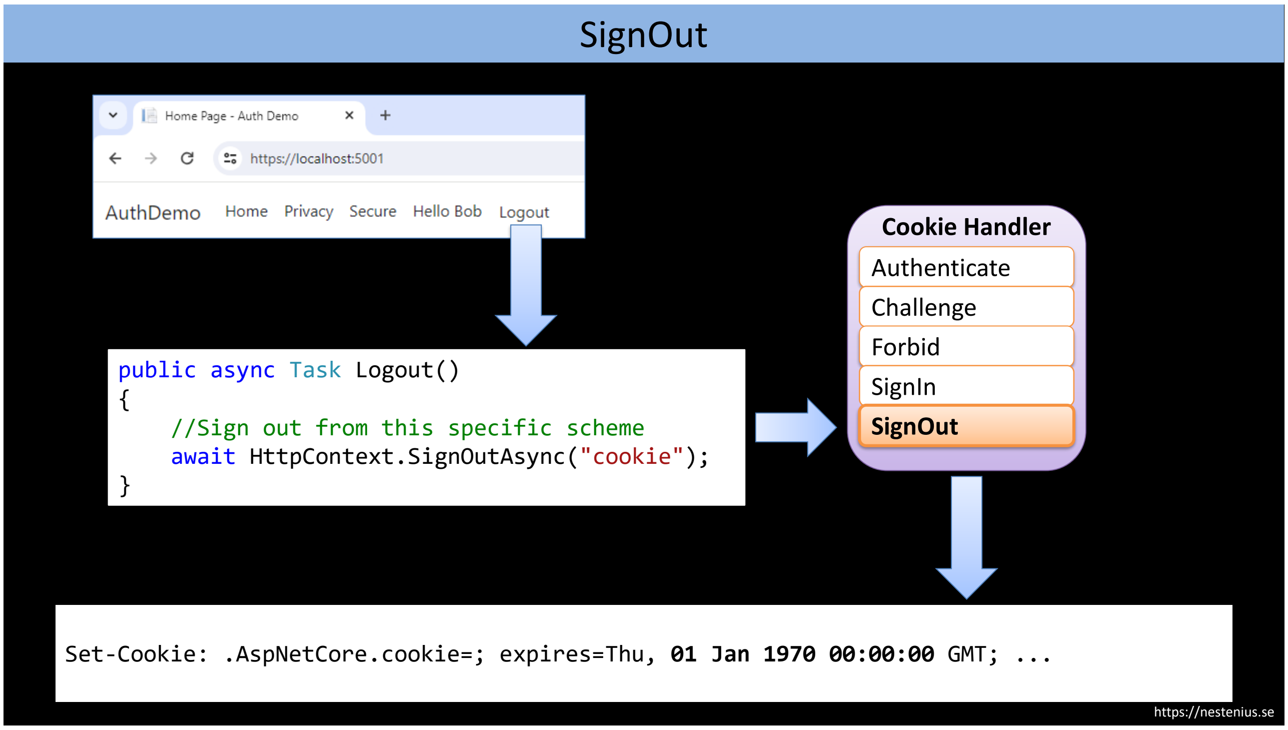
https://nestenius.se

49

Insecure SignOut

https://nestenius.se

50



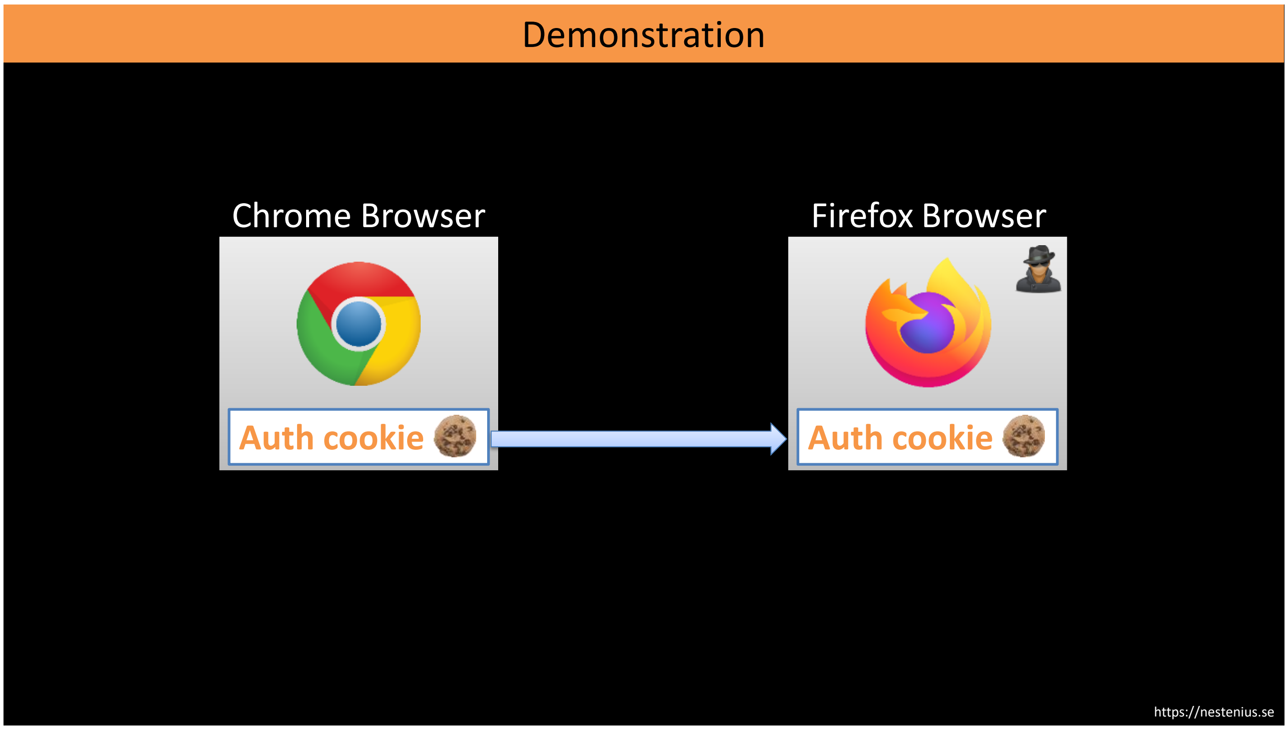
SignOut

```
public async Task Logout()
{
    //Sign out from this specific scheme
    await HttpContext.SignOutAsync("cookie");
}
```

```
Set-Cookie: .AspNetCore.cookie=; expires=Thu, 01 Jan 1970 00:00:00 GMT; ...
```

https://nestenius.se

51



Demonstration

https://nestenius.se

52

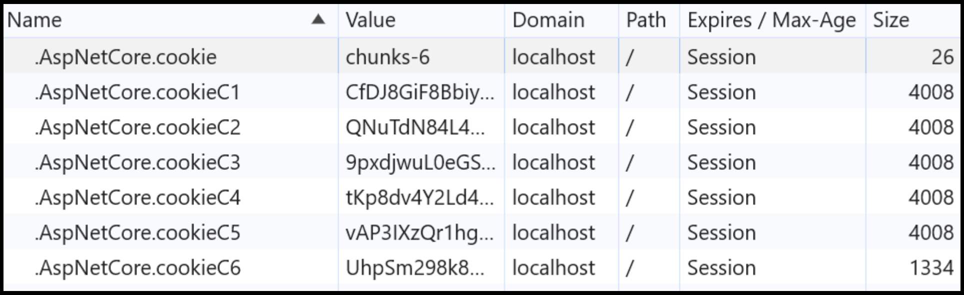
Large Cookies

https://nestenius.se

53

Large Cookies

Multiple cookies may be used to store the data



Name ▲	Value	Domain	Path	Expires / Max-Age	Size
.AspNetCore.cookie	chunks-6	localhost	/	Session	26
.AspNetCore.cookieC1	CfDJ8GiF8Bbiy...	localhost	/	Session	4008
.AspNetCore.cookieC2	QNuTdN84L4...	localhost	/	Session	4008
.AspNetCore.cookieC3	9pxdjwuL0eGS...	localhost	/	Session	4008
.AspNetCore.cookieC4	tKp8dv4Y2Ld4...	localhost	/	Session	4008
.AspNetCore.cookieC5	vAP3IXzQr1hg...	localhost	/	Session	4008
.AspNetCore.cookieC6	UhpSm298k8...	localhost	/	Session	1334

Can we improve this? Yes, we explore this later!

https://nestenius.se

54

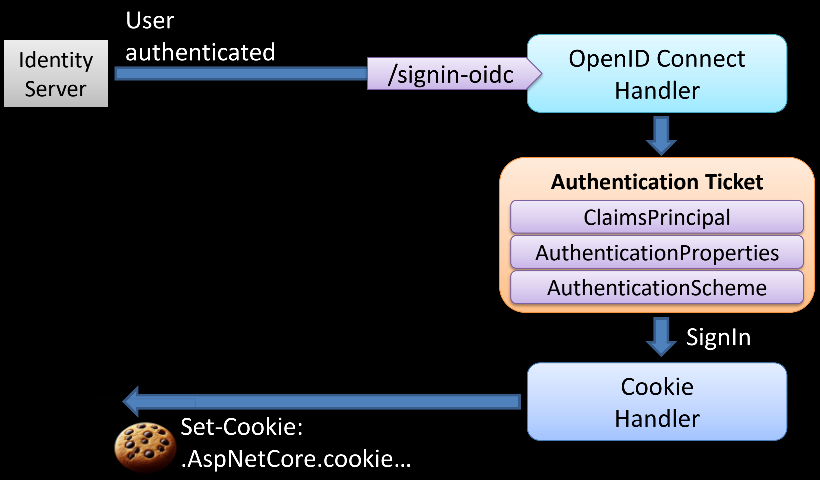
Putting Your Cookies On A Diet

https://nestenius.se

55

Putting Your Cookies On A Diet

The authentication stack so far

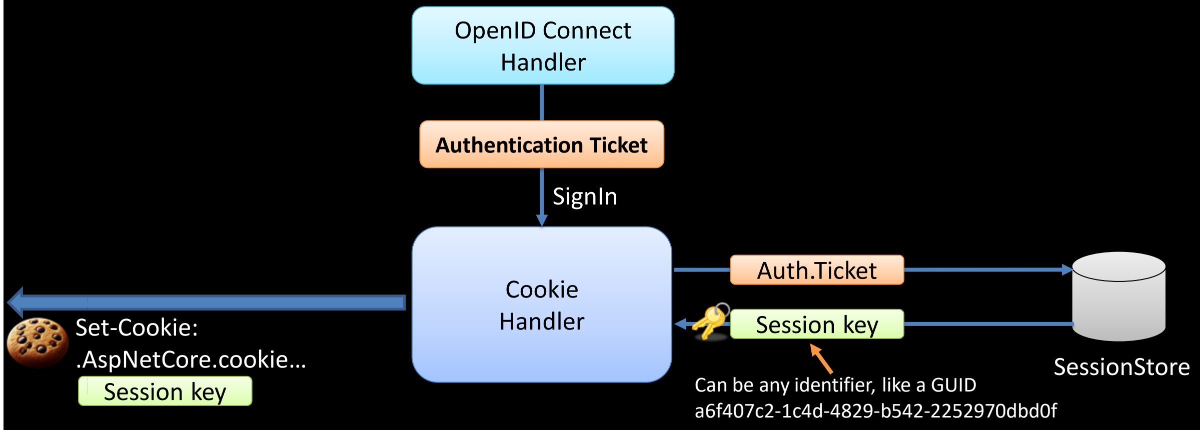


https://nestenius.se

56

Putting Your Cookies On A Diet

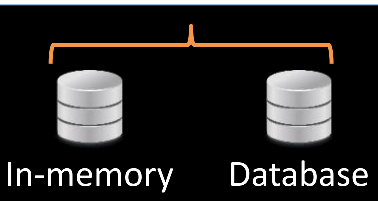
We can add a cookie **SessionStore**



https://nestenius.se

Putting Your Cookies On A Diet

```
public interface ITicketStore
{
    Task<string>                StoreAsync(AuthenticationTicket ticket);
    Task                        RenewAsync(string key, AuthenticationTicket ticket);
    Task<AuthenticationTicket>  RetrieveAsync(string key);
    Task                        RemoveAsync(string key);
}
```



https://nestenius.se

Demonstration – Minimalistic SessionStore

```
public class MySessionStore : ITicketStore
{
    private readonly ConcurrentDictionary<string, AuthenticationTicket> mytickets = new();

    public async Task RemoveAsync(string key)
    {
        if (mytickets.ContainsKey(key))
            mytickets.TryRemove(key, out _);
    }

    public async Task RenewAsync(string key, AuthenticationTicket ticket)
    {
        mytickets[key] = ticket;
    }

    public async Task<AuthenticationTicket> RetrieveAsync(string key)
    {
        return mytickets.TryGetValue(key, out var ticket) ? ticket : default;
    }

    public async Task<string> StoreAsync(AuthenticationTicket ticket)
    {
        var key = Guid.NewGuid().ToString();
        if (mytickets.TryAdd(key, ticket))
            return key;
        else
            throw new Exception("Failed to add entry to MySessionStore");
    }
}
```

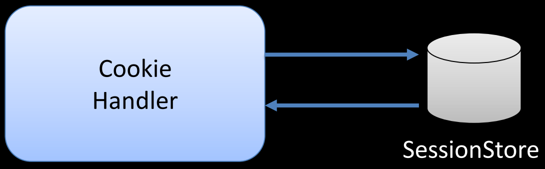
```
.AddCookie("cookie", o =>
{
    o.SessionStore = new MySessionStore();
```

This also solves the SignOut issue

https://nestenius.se

59

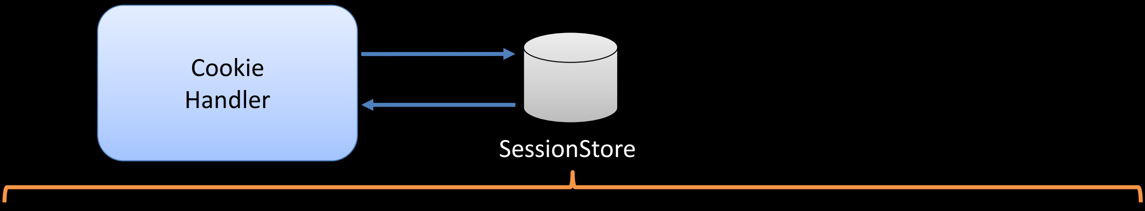
Possibilities using a Session Store

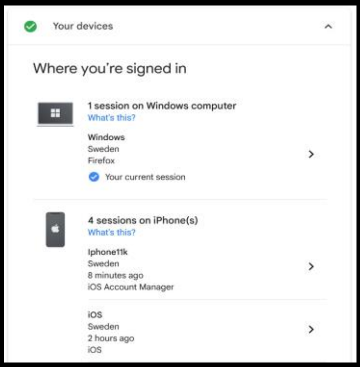


https://nestenius.se

60

Possibilities using a Session Store



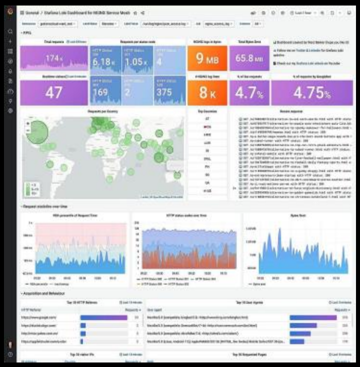

Your devices

Where you're signed in

1 session on Windows computer
What's this?
Windows
Sweden
Firefox
Your current session

4 sessions on iPhone(s)
What's this?
Iphone11k
Sweden
8 minutes ago
iOS Account Manager

iOS
Sweden
2 hours ago
iOS

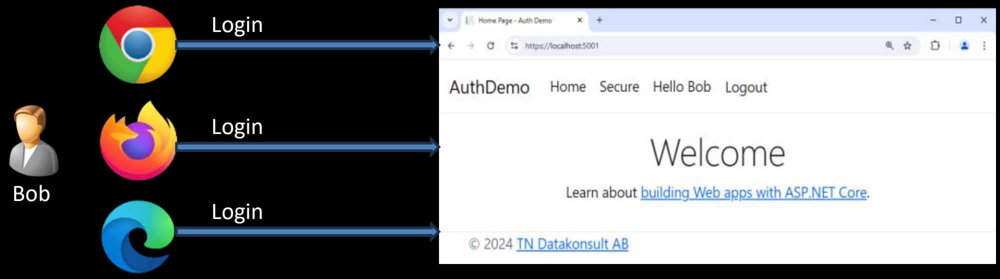


https://nestenius.se

61

Demonstration – Advanced SessionStore

```
.AddCookie("cookie", o =>
{
   ...
   o.SessionStore = new AdvancedSessionStore();

})
```



https://nestenius.se

62

Insecure Redirects

https://nestenius.se

63

Insecure Redirect

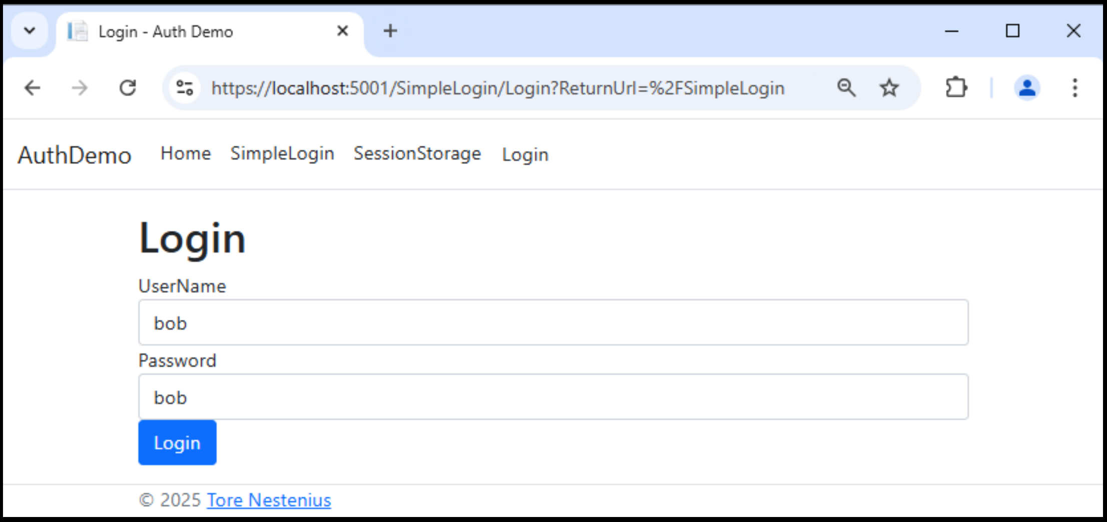
What is the problem?

```
[HttpPost]
[ValidateAntiForgeryToken]
public async Task<IActionResult> Login(LoginModel loginCredentials)
{
    var claims = new List<Claim>()
        { new("sub","1234"), new("name","Bob")};

    var identity = new ClaimsIdentity(claims, "pwd");
    var principal = new ClaimsPrincipal(identity);

    await HttpContext.SignInAsync(scheme: "cookie", principal);

    return Redirect(loginCredentials.ReturnUrl);
}
```

https://nestenius.se

64

Demonstration – Introducing LocalRedirect


Login - Auth Demo

https://localhost:5001/SimpleLogin/Login?ReturnUrl=%2FSimpleLogin

AuthDemo Home SimpleLogin SessionStorage Login

Login

UserName

bob

Password

bob

Login

© 2025 Tore Nestenius

```
return LocalRedirect(loginCredentials.ReturnUrl);
```

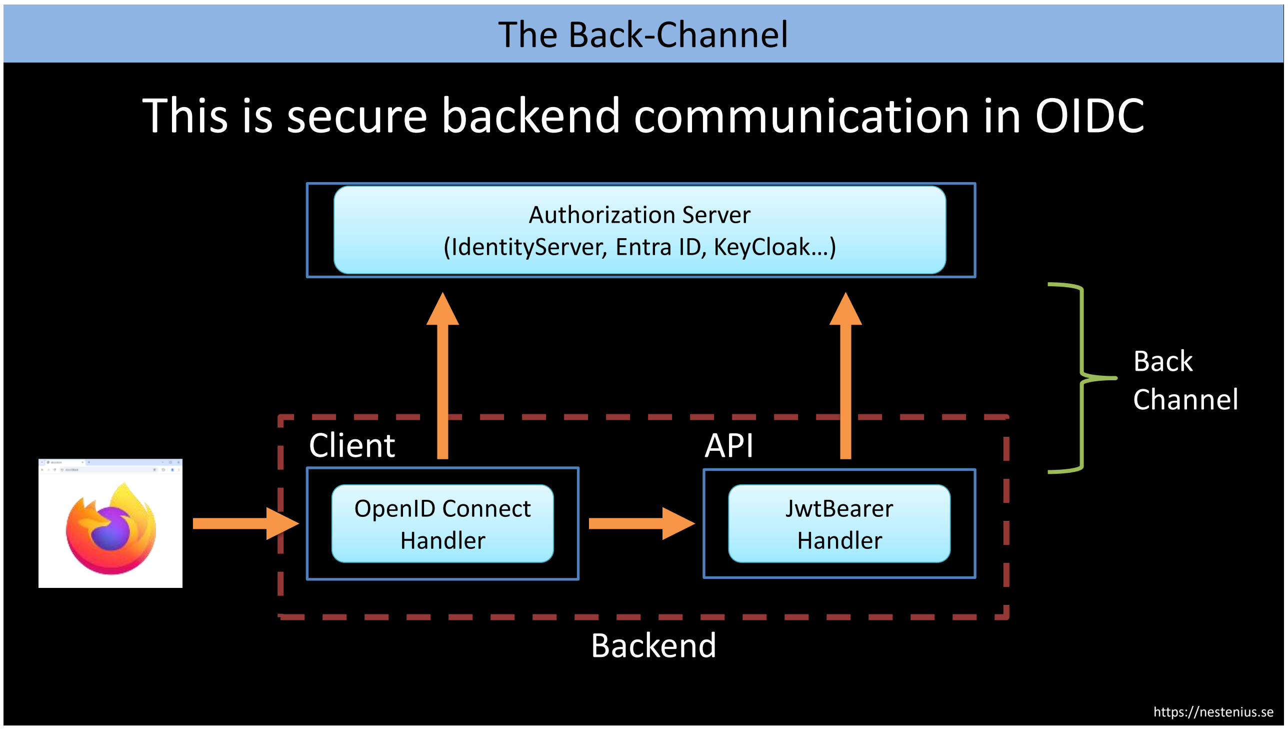
https://nestenius.se

65

The Back-Channel

https://nestenius.se

66

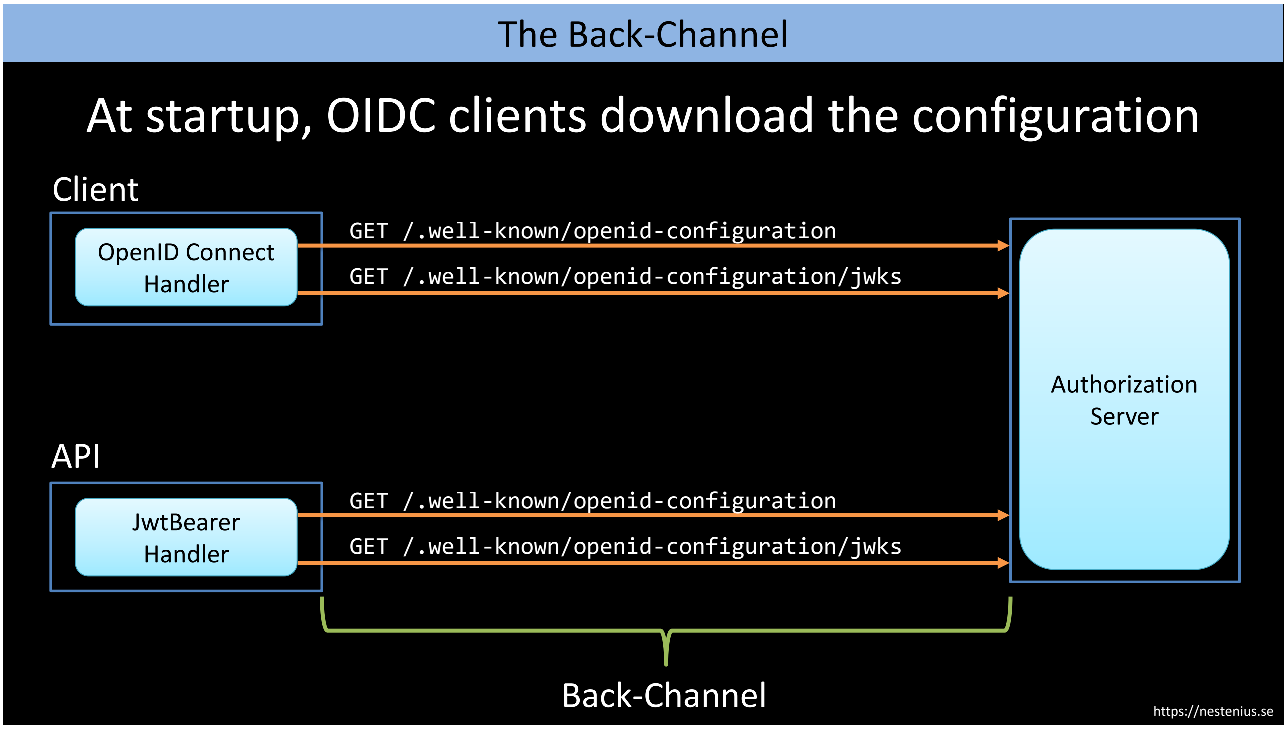


The Back-Channel

This is secure backend communication in OIDC

https://nestenius.se

67



The Back-Channel

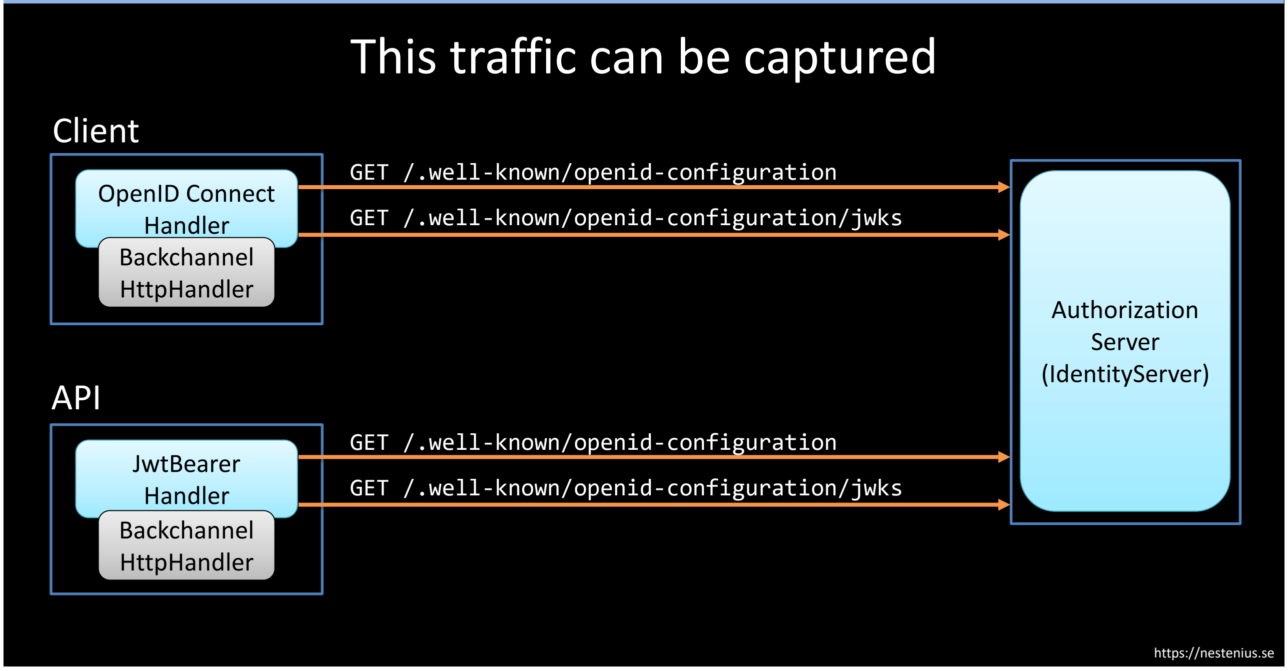
At startup, OIDC clients download the configuration

Client
OpenID Connect Handler
GET /.well-known/openid-configuration
GET /.well-known/openid-configuration/jwks
API
JwtBearer Handler
GET /.well-known/openid-configuration
GET /.well-known/openid-configuration/jwks
Authorization Server
Back-Channel

https://nestenius.se

68

The Back-Channel


This traffic can be captured
Client
OpenID Connect Handler
Backchannel HttpHandler
GET /.well-known/openid-configuration
GET /.well-known/openid-configuration/jwks
API
JwtBearer Handler
Backchannel HttpHandler
GET /.well-known/openid-configuration
GET /.well-known/openid-configuration/jwks
Authorization Server (IdentityServer)
https://nestenius.se

69

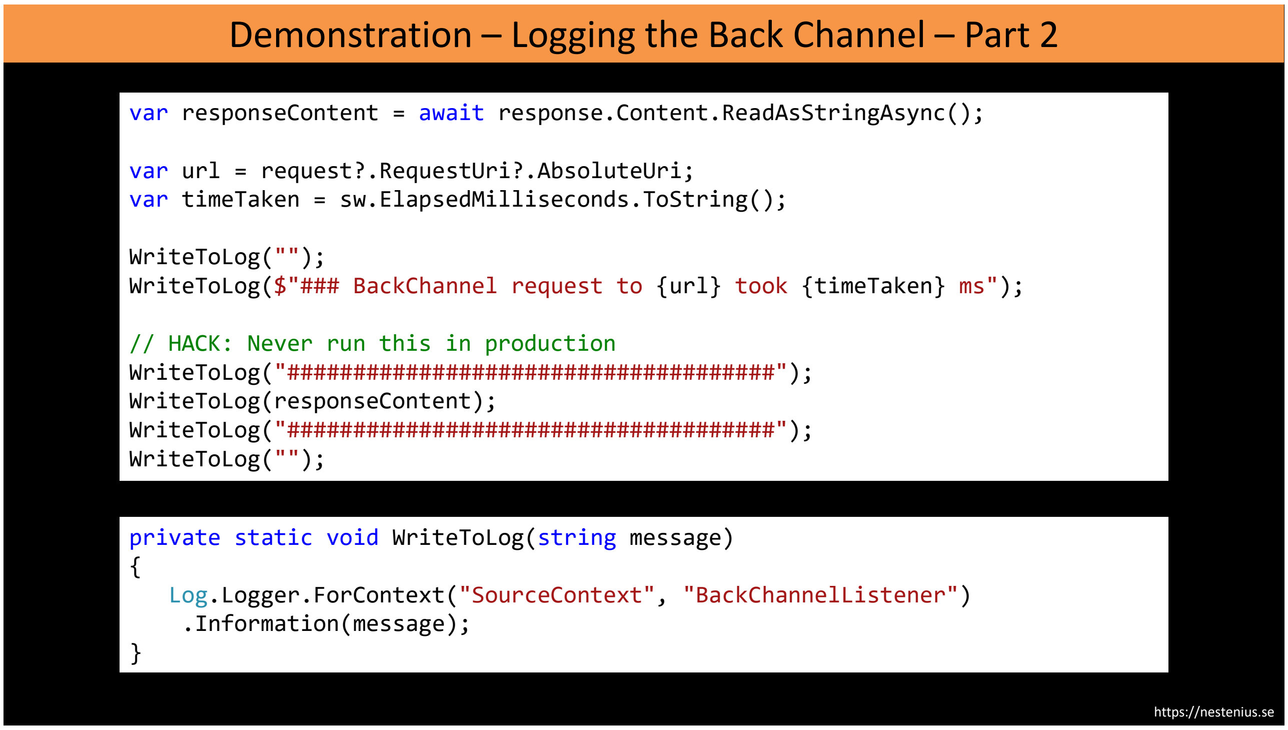
Demonstration – Logging the Back-Channel

```
public class BackChannelListener : DelegatingHandler
{
    public BackChannelListener() : base(new HttpClientHandler())
    { }

    protected async override Task<HttpResponseMessage> SendAsync(HttpRequestMessage request,
                                                                 CancellationToken token)
    {
        var sw = new Stopwatch();
        sw.Start();

        var response = await base.SendAsync(request, token);

        sw.Stop();

        // TODO...

        return response;
    }
}
```

```
o.BackchannelHttpHandler = new BackChannelListener();
```

https://nestenius.se

70



Demonstration – Logging the Back Channel – Part 2

```
var responseContent = await response.Content.ReadAsStringAsync();

var url = request?.RequestUri?.AbsoluteUri;
var timeTaken = sw.ElapsedMilliseconds.ToString();

WriteToLog("");
WriteToLog($"### BackChannel request to {url} took {timeTaken} ms");

// HACK: Never run this in production
WriteToLog("######################################");
WriteToLog(responseContent);
WriteToLog("######################################");
WriteToLog("");
```

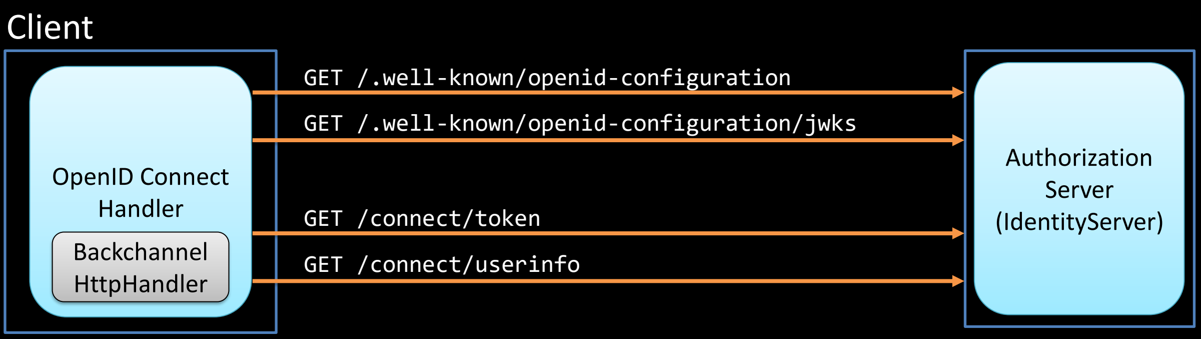
```
private static void WriteToLog(string message)
{
   Log.Logger.ForContext("SourceContext", "BackChannelListener")
    .Information(message);
}
```

https://nestenius.se

71

Demonstration – Logging the Back-Channel – Part 3

We will see the following requests in the output

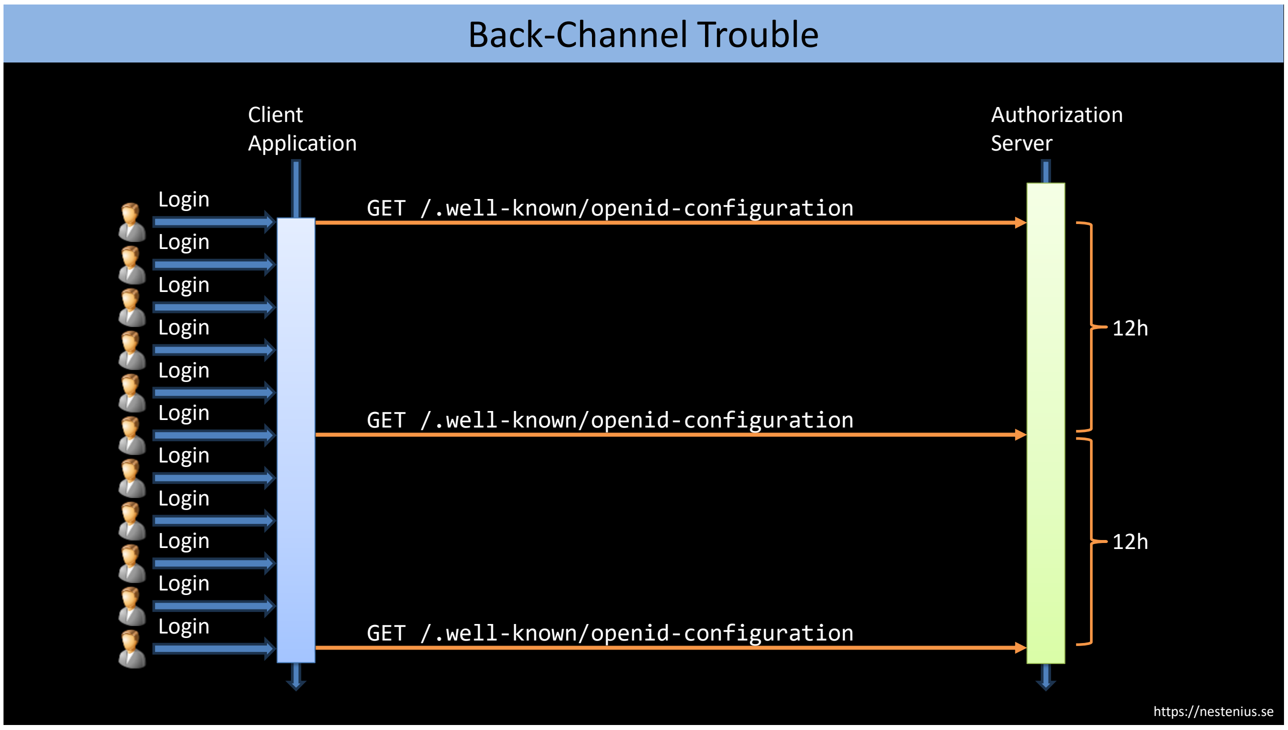

Client
OpenID Connect Handler
Backchannel HttpHandler
GET /.well-known/openid-configuration
GET /.well-known/openid-configuration/jwks
GET /connect/token
GET /connect/userinfo
Authorization Server (IdentityServer)

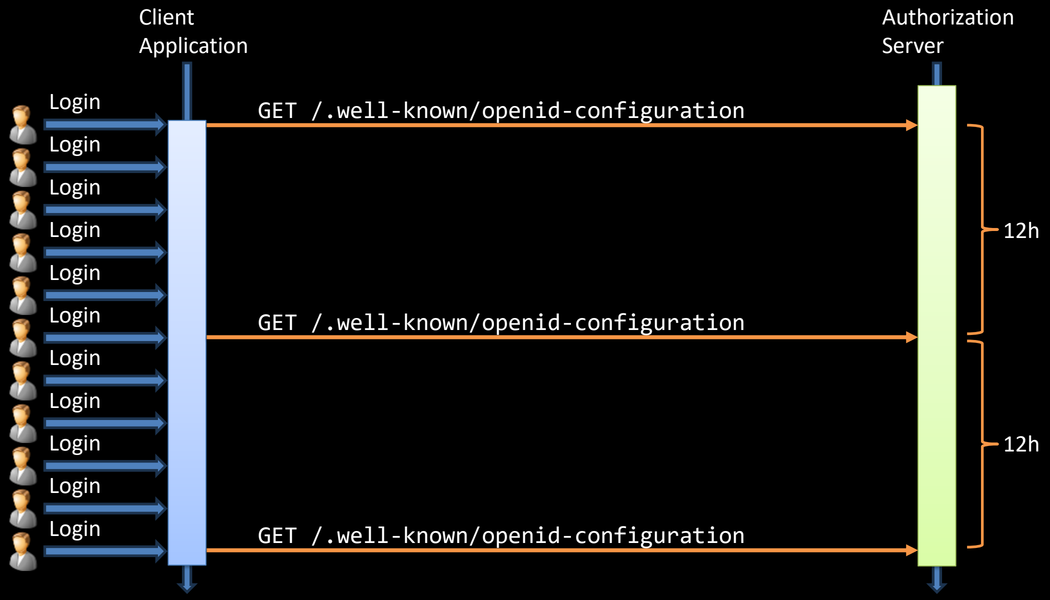
https://nestenius.se

72

Back-Channel Trouble

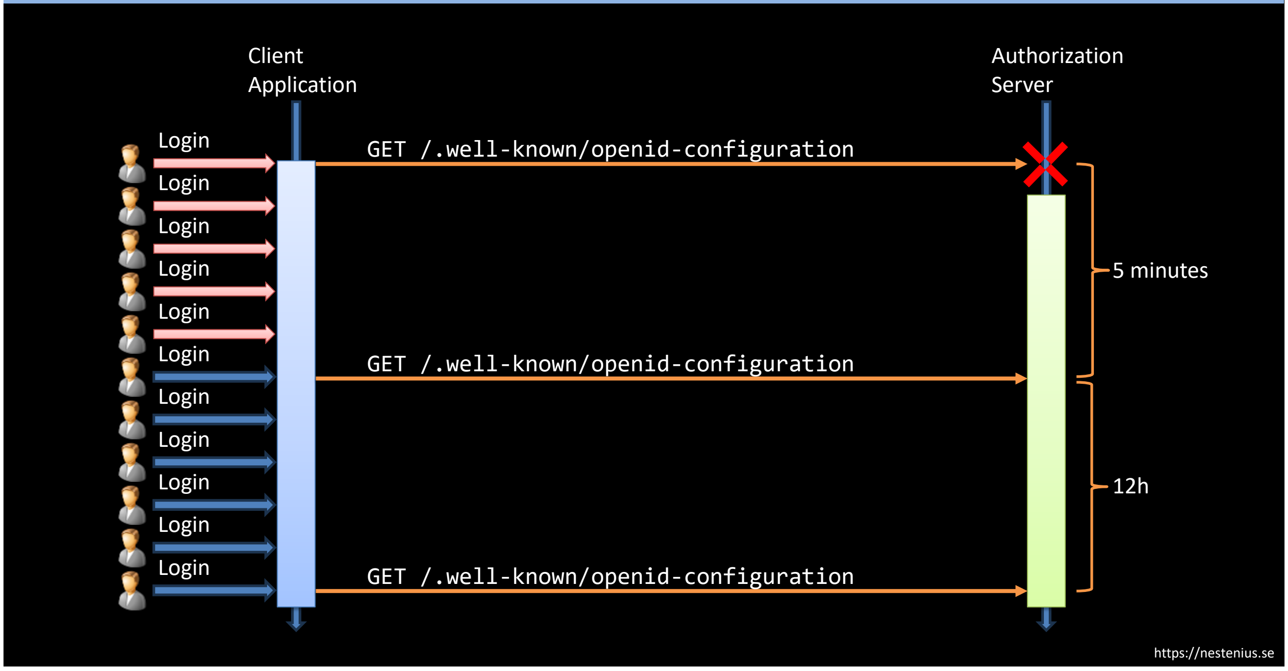
https://nestenius.se


Back-Channel Trouble

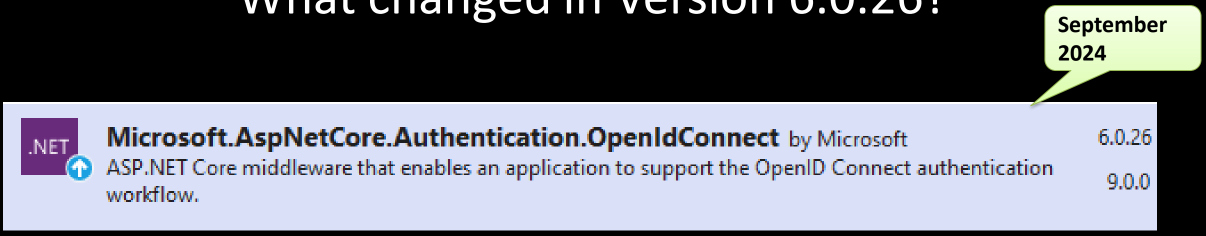

Client Application
Authorization Server
Login
Login
Login
Login
Login
Login
Login
Login
Login
Login
Login
GET /.well-known/openid-configuration
GET /.well-known/openid-configuration
GET /.well-known/openid-configuration
12h
12h

https://nestenius.se

Back-Channel Trouble

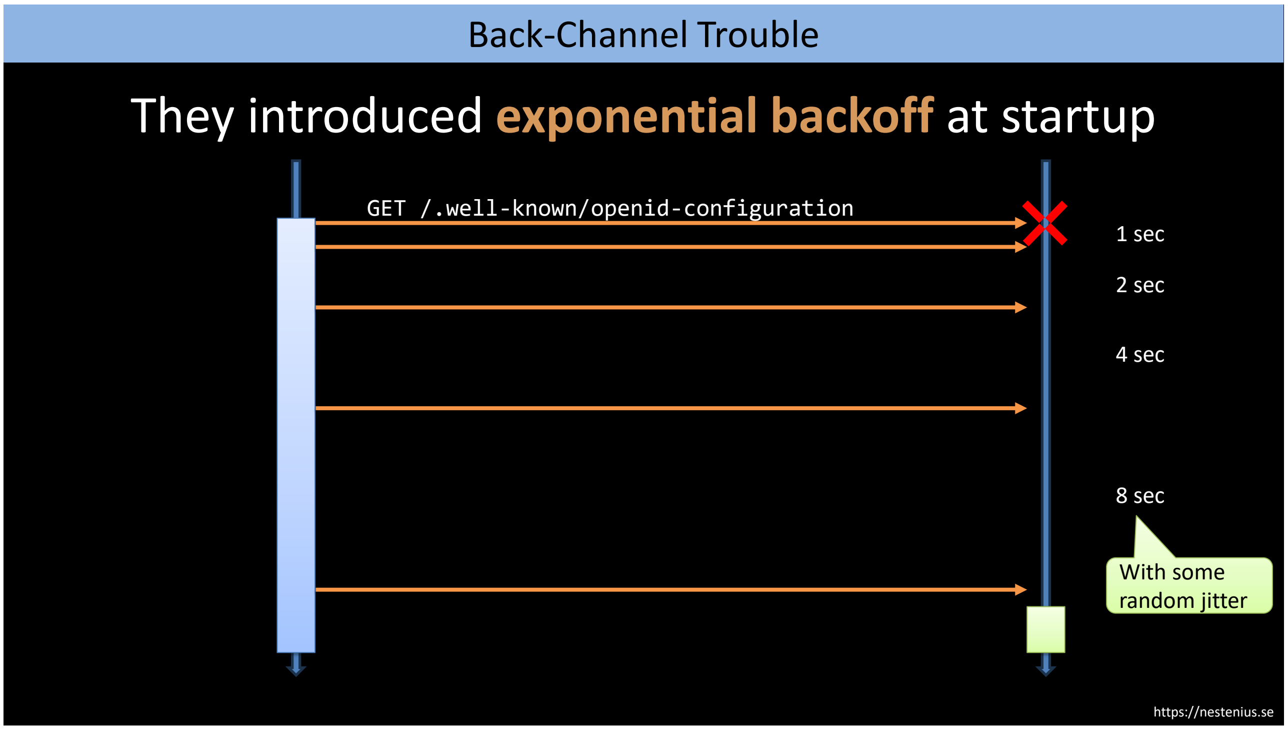


What changed in Version 6.0.26?



Microsoft.AspNetCore.Authentication.OpenIdConnect by Microsoft
ASP.NET Core middleware that enables an application to support the OpenID Connect authentication workflow.
6.0.26
9.0.0

https://nestenius.se

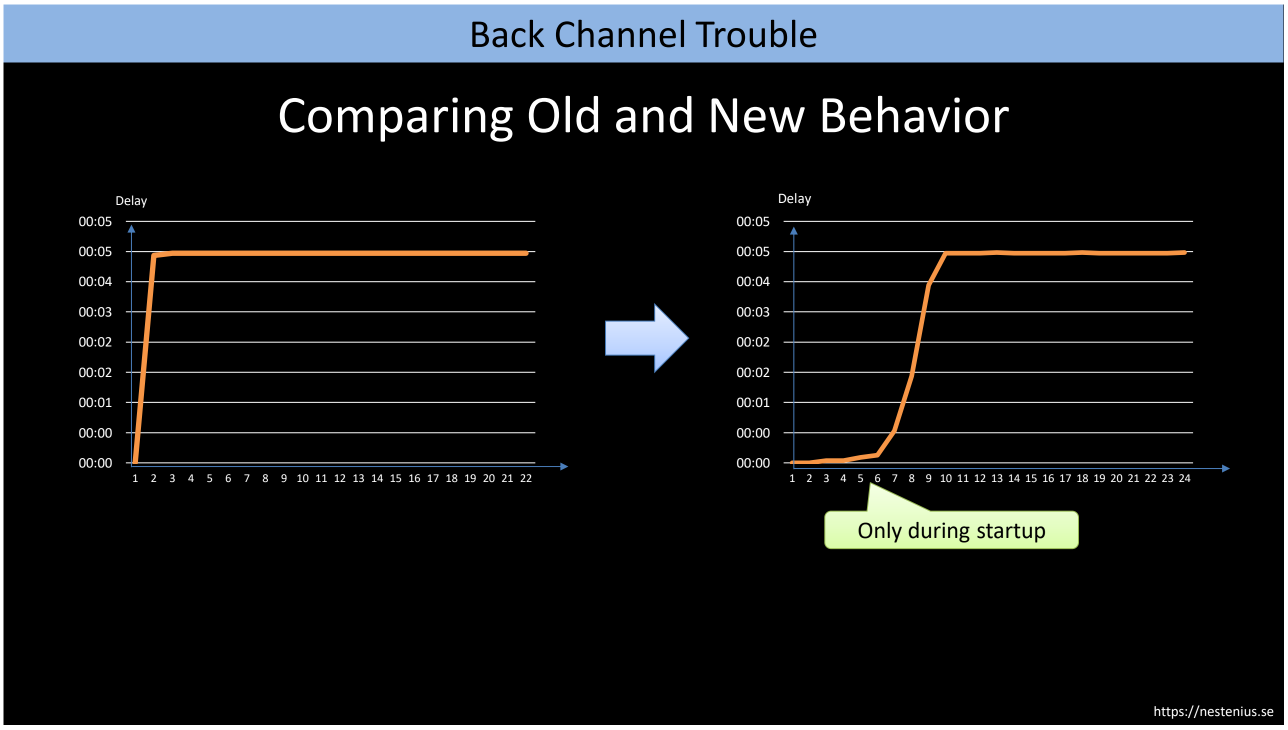


Back-Channel Trouble

They introduced **exponential backoff** at startup

https://nestenius.se

77

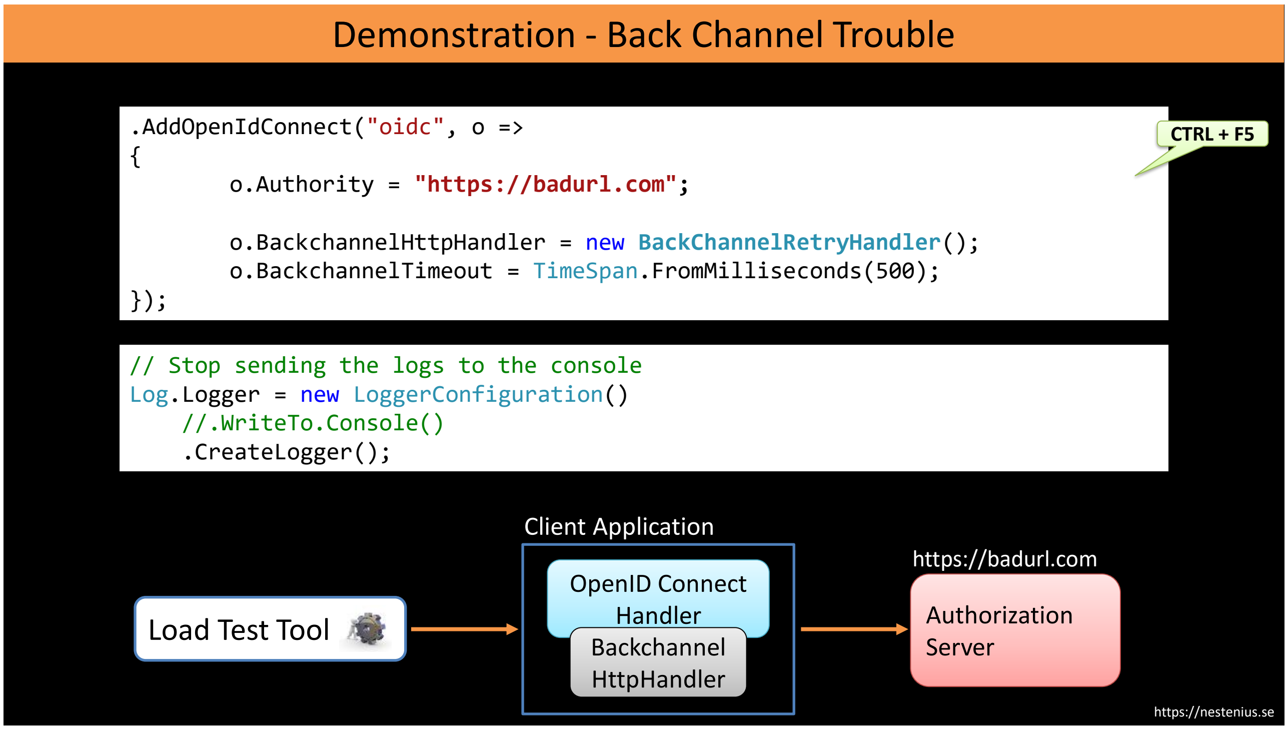


Back Channel Trouble

Comparing Old and New Behavior

https://nestenius.se

78

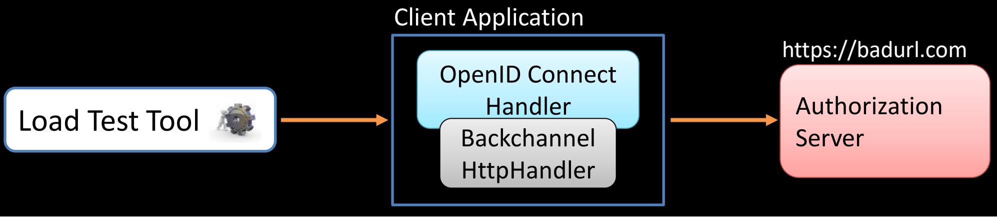


Demonstration - Back Channel Trouble

```
.AddOpenIdConnect("oidc", o =>
{
        o.Authority = "https://badurl.com";

        o.BackchannelHttpHandler = new BackChannelRetryHandler();
        o.BackchannelTimeout = TimeSpan.FromMilliseconds(500);
});
```

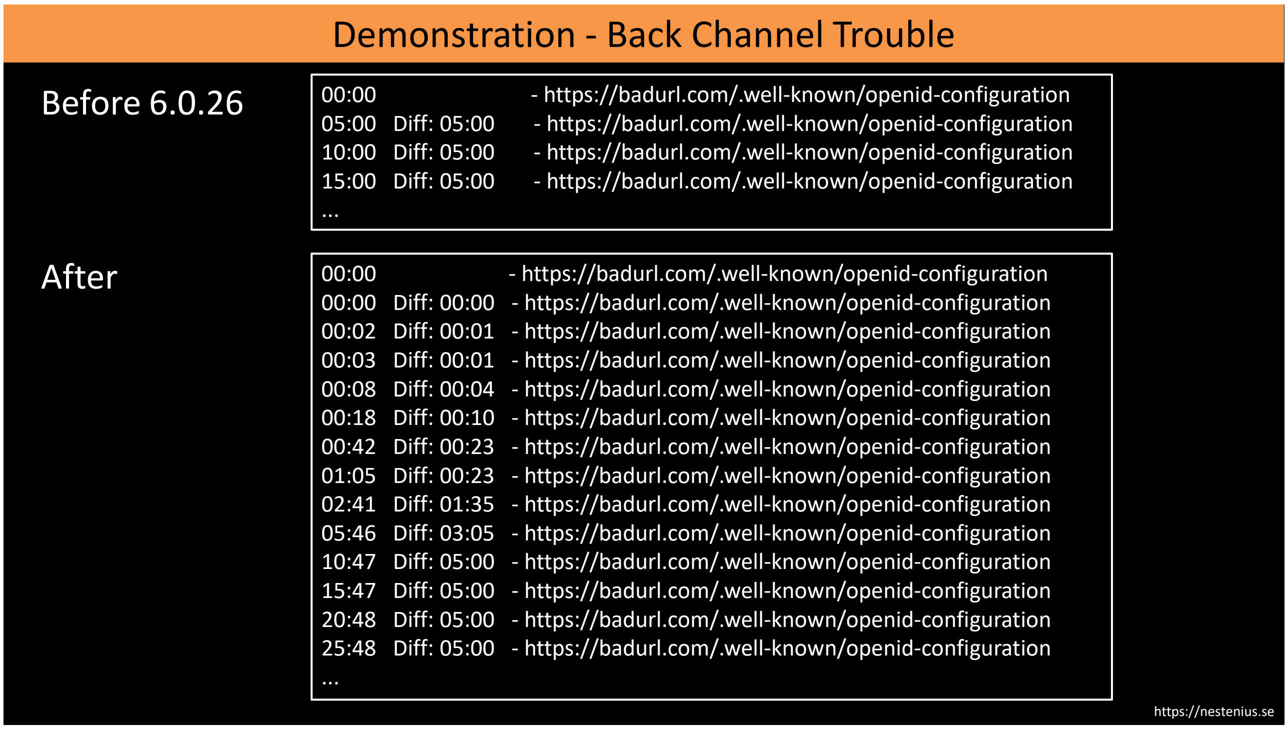
CTRL + F5

```
// Stop sending the logs to the console
Log.Logger = new LoggerConfiguration()
    //.WriteTo.Console()
    .CreateLogger();
```



https://nestenius.se

79



Demonstration - Back Channel Trouble

Before 6.0.26

```
00:00                  - https://badurl.com/.well-known/openid-configuration
05:00   Diff: 05:00    - https://badurl.com/.well-known/openid-configuration
10:00   Diff: 05:00    - https://badurl.com/.well-known/openid-configuration
15:00   Diff: 05:00    - https://badurl.com/.well-known/openid-configuration
...
```

After

```
00:00                - https://badurl.com/.well-known/openid-configuration
00:00   Diff: 00:00  - https://badurl.com/.well-known/openid-configuration
00:02   Diff: 00:01  - https://badurl.com/.well-known/openid-configuration
00:03   Diff: 00:01  - https://badurl.com/.well-known/openid-configuration
00:08   Diff: 00:04  - https://badurl.com/.well-known/openid-configuration
00:18   Diff: 00:10  - https://badurl.com/.well-known/openid-configuration
00:42   Diff: 00:23  - https://badurl.com/.well-known/openid-configuration
01:05   Diff: 00:23  - https://badurl.com/.well-known/openid-configuration
02:41   Diff: 01:35  - https://badurl.com/.well-known/openid-configuration
05:46   Diff: 03:05  - https://badurl.com/.well-known/openid-configuration
10:47   Diff: 05:00  - https://badurl.com/.well-known/openid-configuration
15:47   Diff: 05:00  - https://badurl.com/.well-known/openid-configuration
20:48   Diff: 05:00  - https://badurl.com/.well-known/openid-configuration
25:48   Diff: 05:00  - https://badurl.com/.well-known/openid-configuration
...
```

https://nestenius.se

80

§

The end!

Would you like me to present this at your company for free?

Presentation and code
https://github.com/tndataab/PublicBlogContent

Blog
https://nestenius.se

Work
https://tn-data.se

https://nestenius.se

81