Exploring Authentication in ASP.NET Core

nestenius.se

MVP Microsoft Most Valuable Professional

https://nestenius.se

1

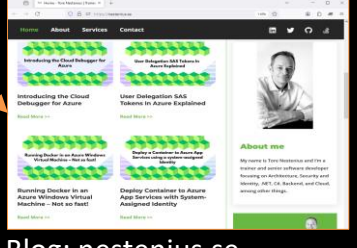
About Tore Nestenius

Tore

Work: tn-data.se

Training and consulting

- OpenID Connect
- IdentityServer
- .NET
- Security
- …



Blog: nestenius.se

https://nestenius.se

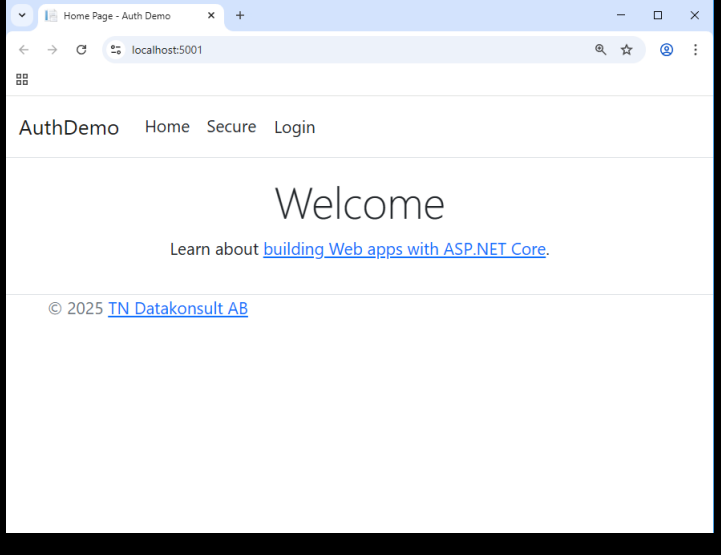
2

Sample Application

https://nestenius.se

5

The Sample Application



https://nestenius.se

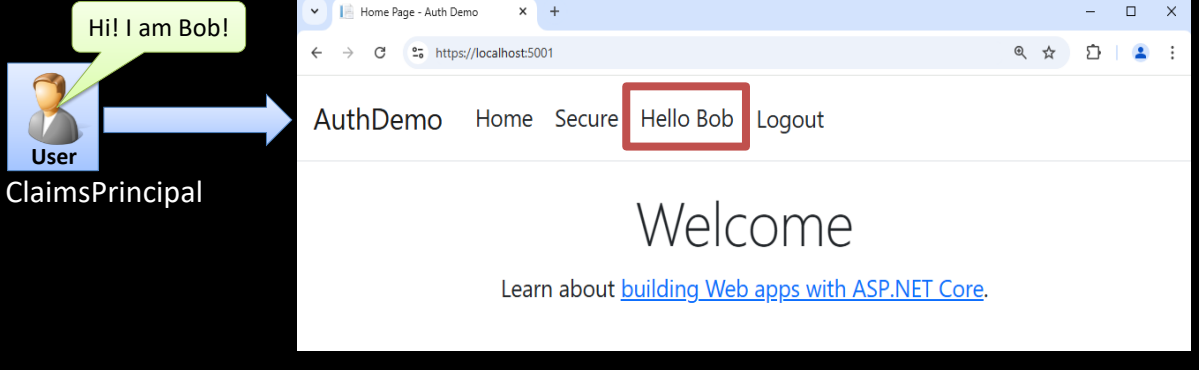
6

What is the goal of this presentation?

https://nestenius.se

7

What does a page need to support this?

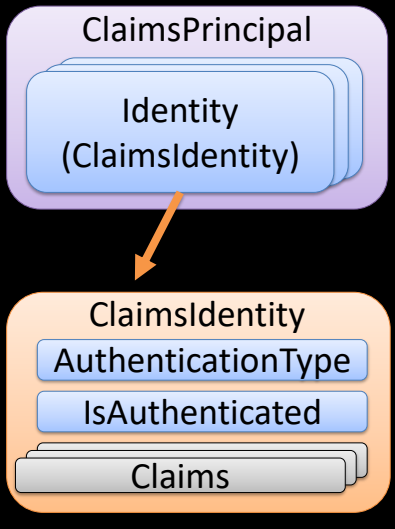



```
<a href="/User/Info">
  Hello @(User?.Identity?.Name ?? "Unknown")
</a>
```

https://nestenius.se

8

ClaimsPrincipal




```
public class ClaimsPrincipal : IPrincipal
{
    //List of identities
    List<ClaimsIdentity> _identities = new();
     ...
}
```

```
public class ClaimsIdentity : IIdentity
{
    //List of claims
    List<Claim> _instanceClaims = new();
    ...
}
```

https://nestenius.se

9

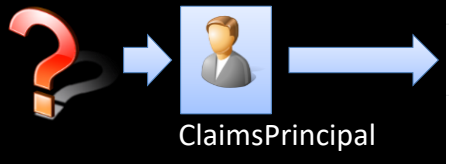
Claims

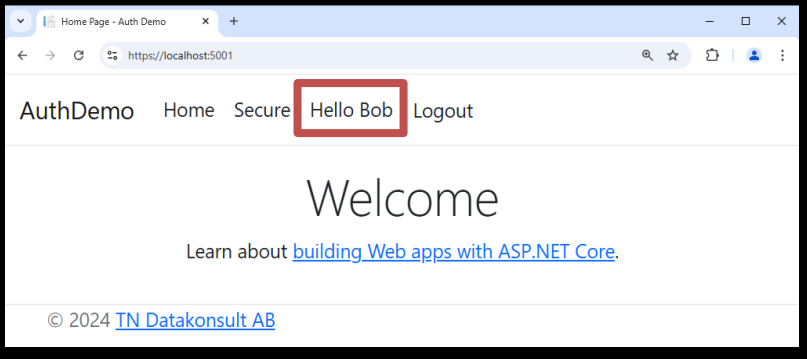
```
var claims = new List<Claim>()
       {
           new("sub","1234"),
           new("name","Bob"),
           new("email","bob@tn-data.se"),
           new("role","developer")
       };
```

https://nestenius.se

10

Who creates the ClaimsPrincipal?





https://nestenius.se

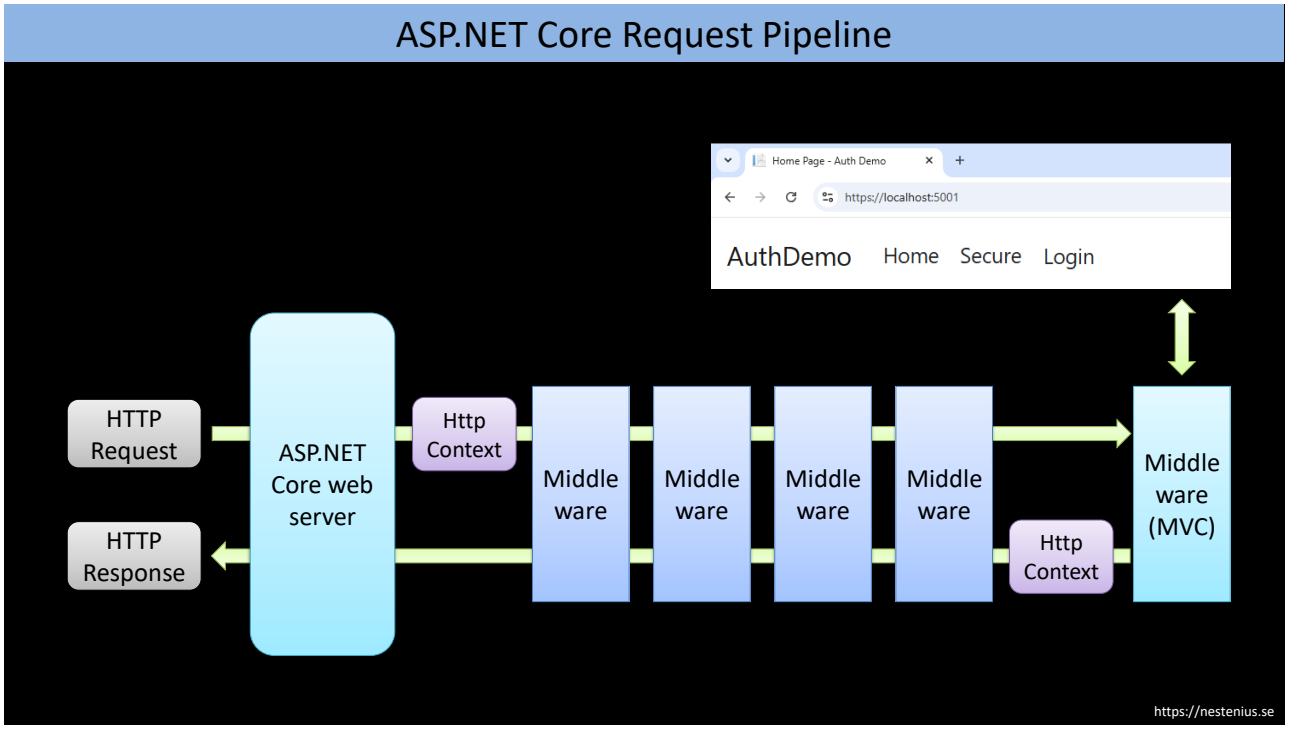
11

ASP.NET Core Request Pipeline

https://nestenius.se

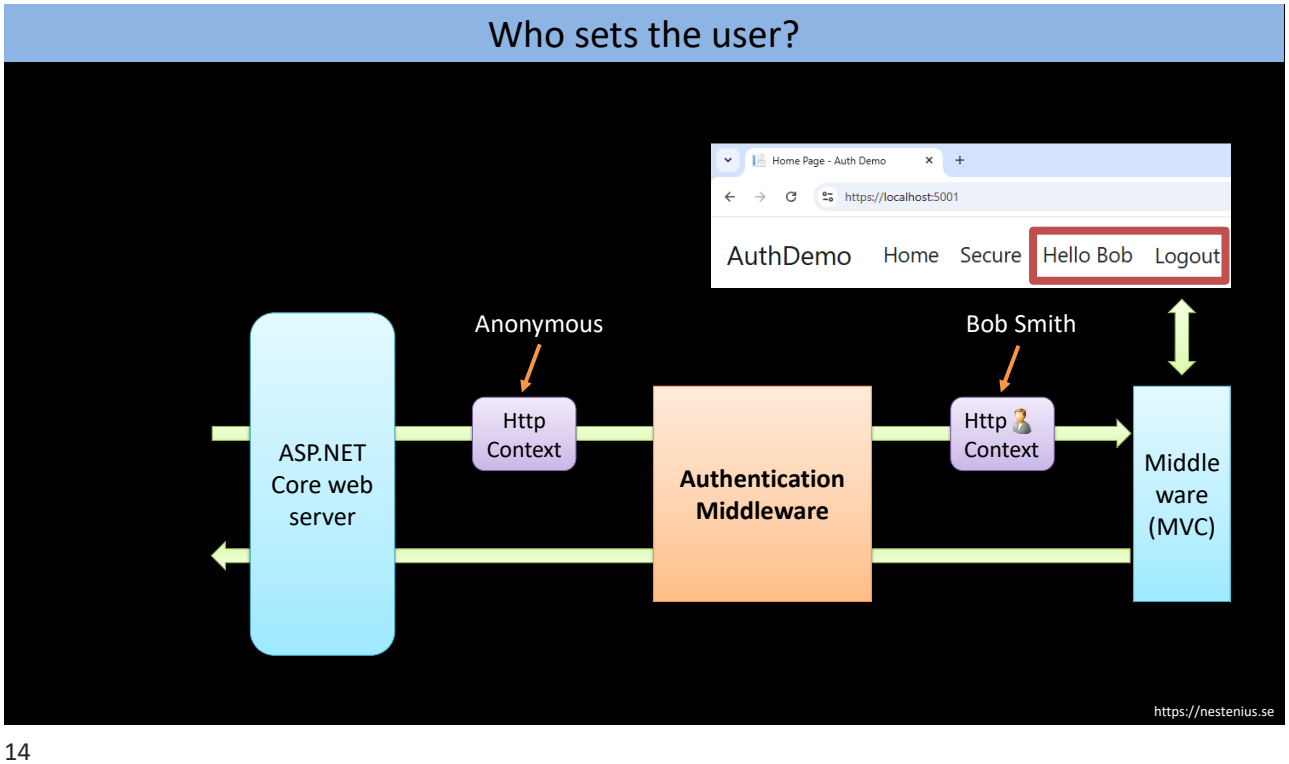
12

ASP.NET Core Request Pipeline



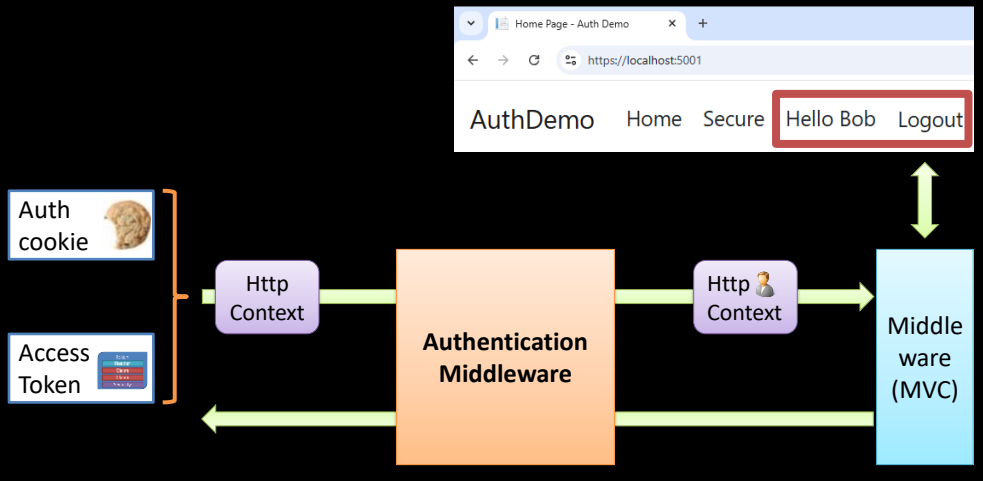
13

Who sets the user?



14

Where does the user data come from?



https://nestenius.se

15

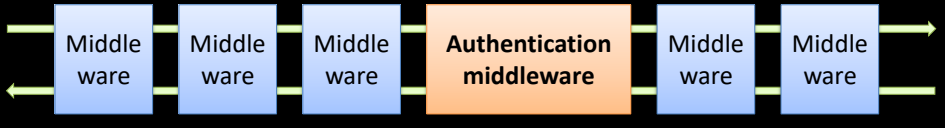
Live coding #1

```
builder.Services.AddAuthentication();

...

app.UseAuthentication();
```

https://nestenius.se

16

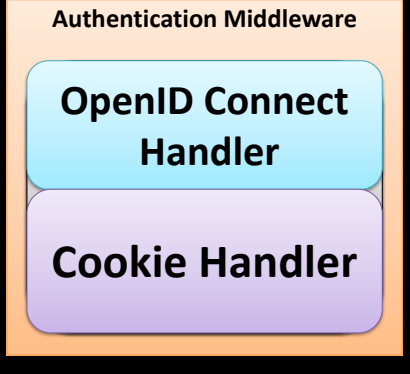
What is inside Authentication?



https://nestenius.se

17

Authentication Handlers




```
//Add the Cookie handler
builder.Services.AddAuthentication()
                .AddCookie();
```

```
// Add the JwtBearer handler (for APIs)
builder.Services.AddAuthentication()
                .AddJwtBearer();
```

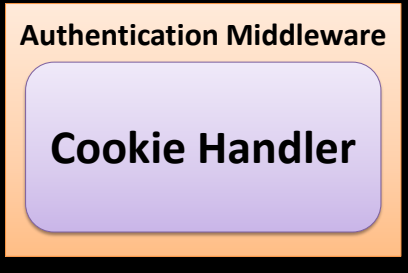
```
//Add the Cookie and OpenID-Connect handler
builder.Services.AddAuthentication()
                .AddCookie()
                .AddOpenIdConnect();
```

https://nestenius.se

18

Live coding #2

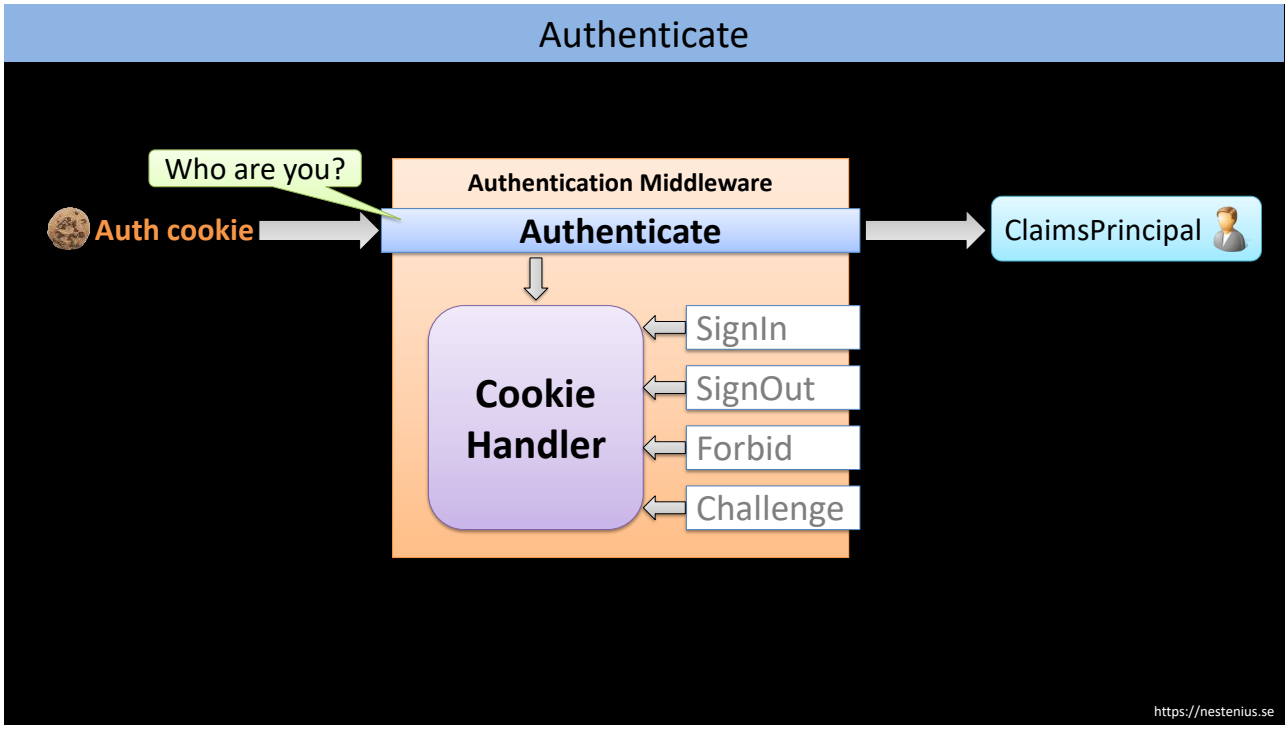
```
builder.Services
       .AddAuthentication()
       .AddCookie(o =>
       {
           o.LoginPath = "/user/login";
           o.LogoutPath = "/user/loggedOut";
           o.AccessDeniedPath = "/user/AccessDenied";
       });
```



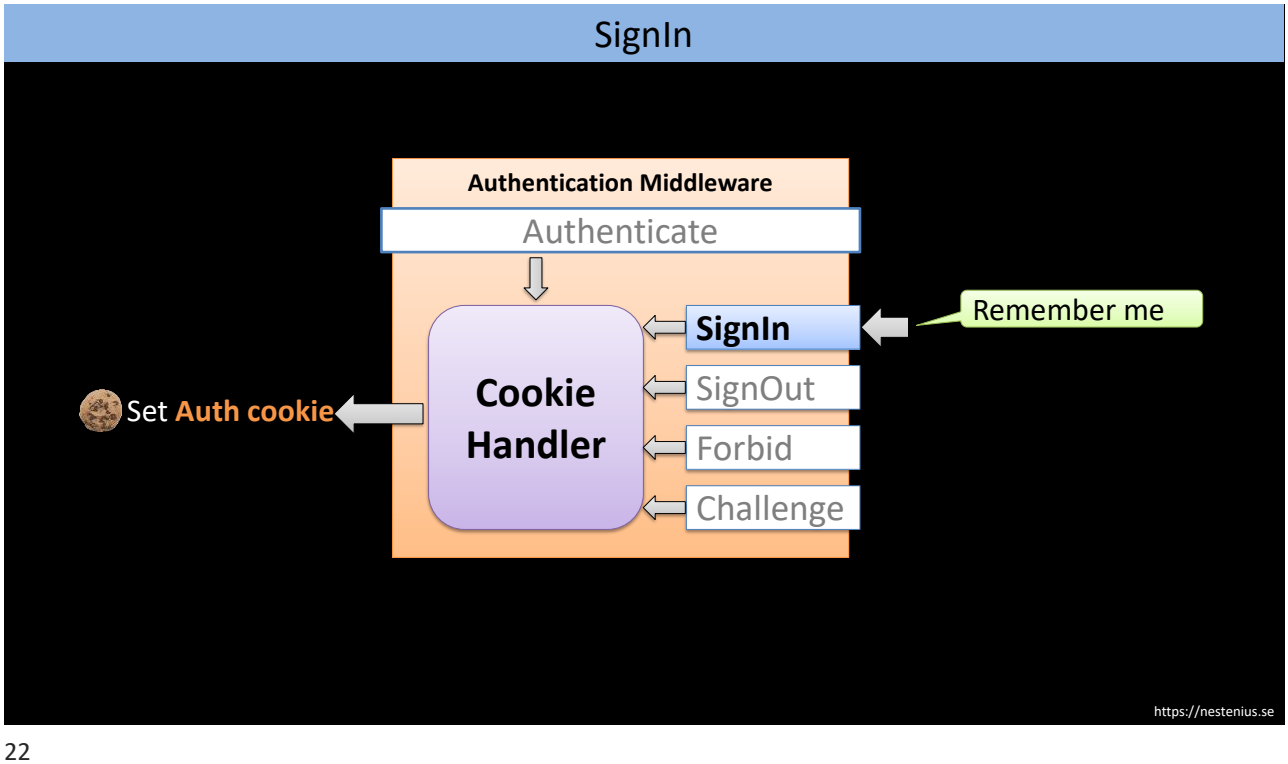
https://nestenius.se

Authentication Operations

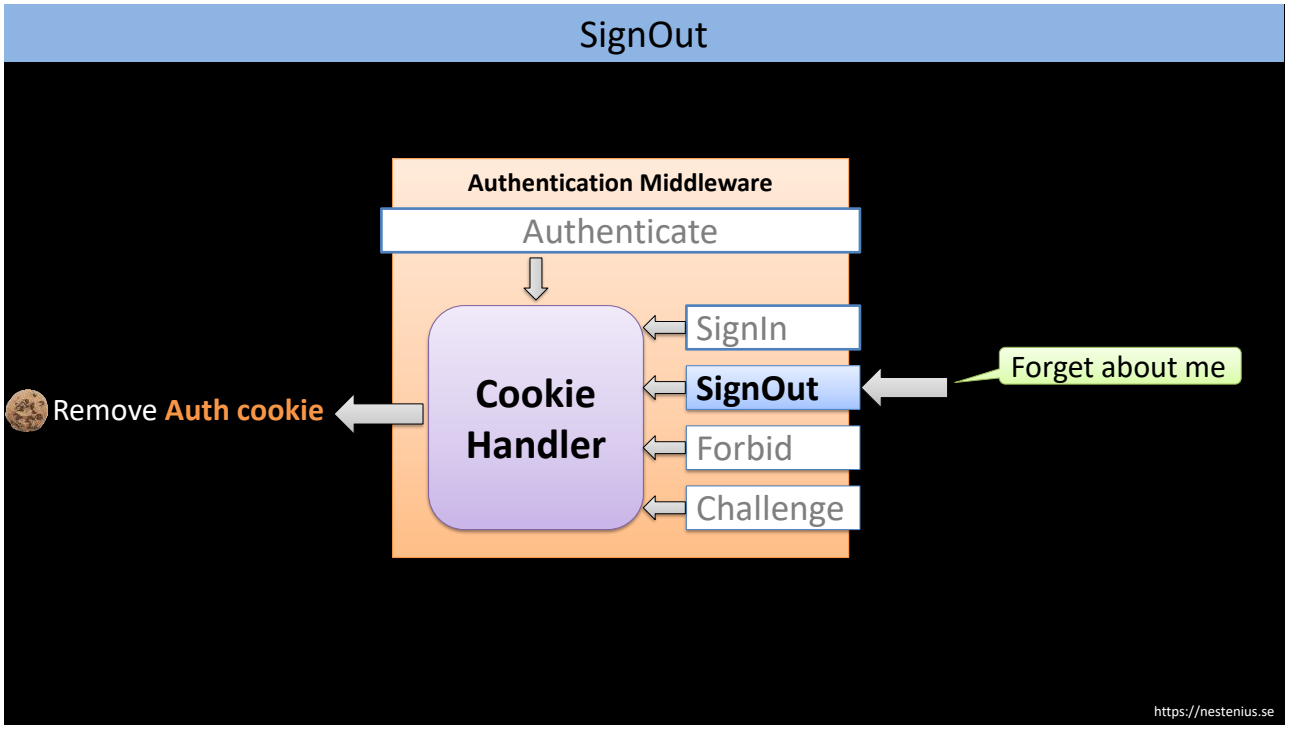
https://nestenius.se


Authenticate
Who are you?
Auth cookie
Authentication Middleware
Authenticate
ClaimsPrincipal
Cookie Handler
SignIn
SignOut
Forbid
Challenge
https://nestenius.se

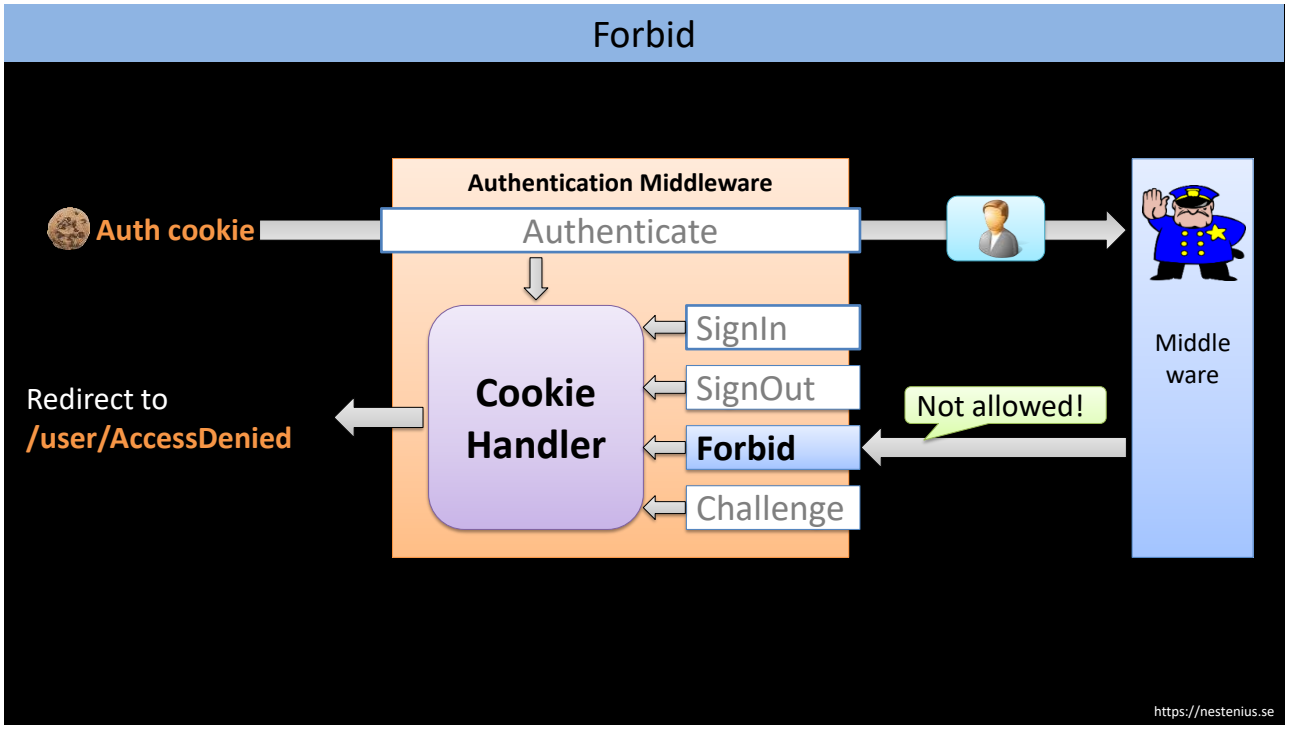
21


SignIn
Authentication Middleware
Authenticate
Remember me
Set Auth cookie
Cookie Handler
SignIn
SignOut
Forbid
Challenge
https://nestenius.se

22

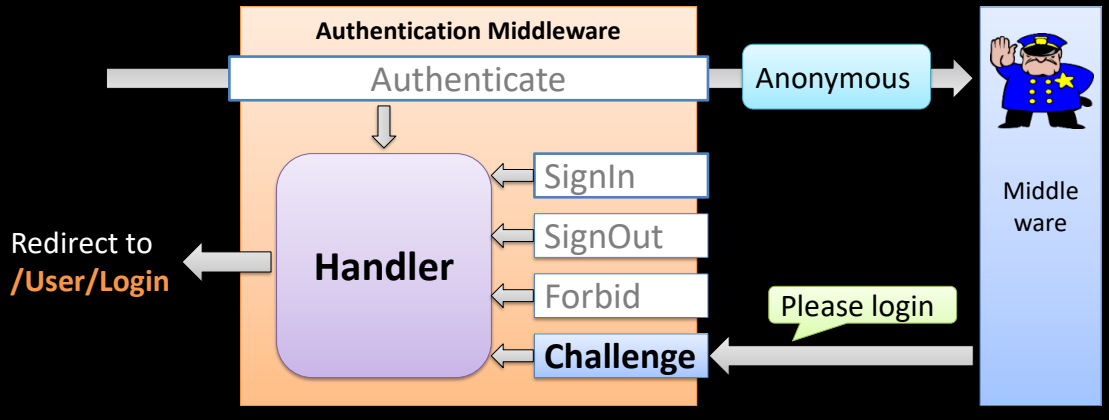

SignOut
Authentication Middleware
Authenticate
Cookie Handler
SignIn
SignOut
Forbid
Challenge
Forget about me
Remove Auth cookie
https://nestenius.se

23


Forbid
Authentication Middleware
Authenticate
Auth cookie
Cookie Handler
SignIn
SignOut
Forbid
Challenge
Redirect to /user/AccessDenied
Not allowed!
Middle ware
https://nestenius.se

24

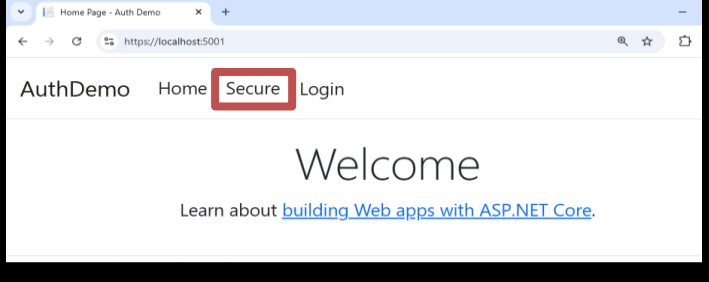
Challenge



https://nestenius.se

25

Live coding #3



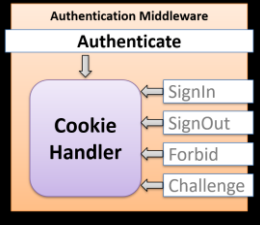
https://localhost:5001/Secure

```
public async Task<IActionResult> Index()
{
    if (User.Identity.IsAuthenticated == false)
        return Challenge();
    else
        return View();
}
```

https://nestenius.se

26

Triggering the Authentication Operations



https://nestenius.se

27

Triggering the Authentication Operations

```
public async Task<IActionResult> Index()
{
    await HttpContext.AuthenticateAsync();
    // or
    await HttpContext.ChallengeAsync();
    // or
    await HttpContext.SignInAsync(...);
    // or
    await HttpContext.SignOutAsync();
    // or
    await HttpContext.ForbidAsync();
}
```

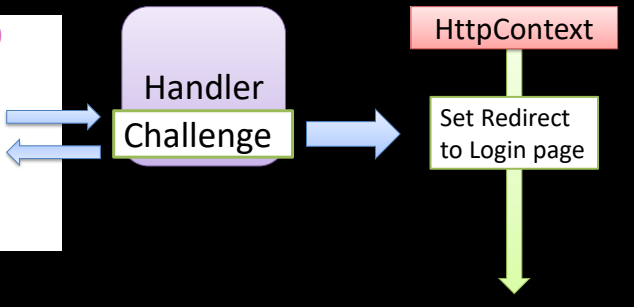
What happens under the hood?

https://nestenius.se

28

Triggering the Authentication Operations

```
public async Task<IActionResult> Index()
{
    // ...
    await HttpContext.ChallengeAsync();
    // ...
}
```



What is the other approach?

https://nestenius.se

29

Triggering the Authentication Operations

```
public IActionResult Index()
{
    // ...
    return Challenge();
    // or
    return SignIn(...);
    // or
    return SignOut();
    // or
    return Forbid();
}
```

```
public IActionResult Index()
{
    return Challenge();
}
```

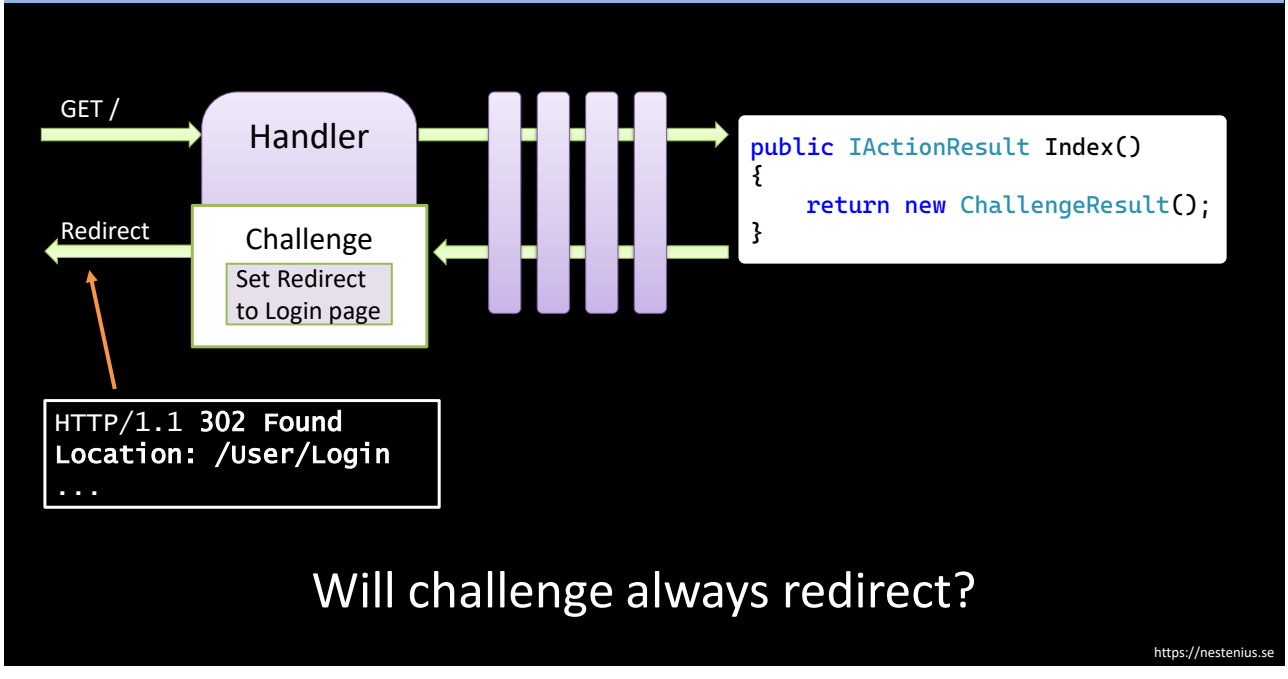
```
public IActionResult Index()
{
    return new ChallengeResult();
}
```

What happens when we do this?

https://nestenius.se

30

Triggering the Authentication Operations

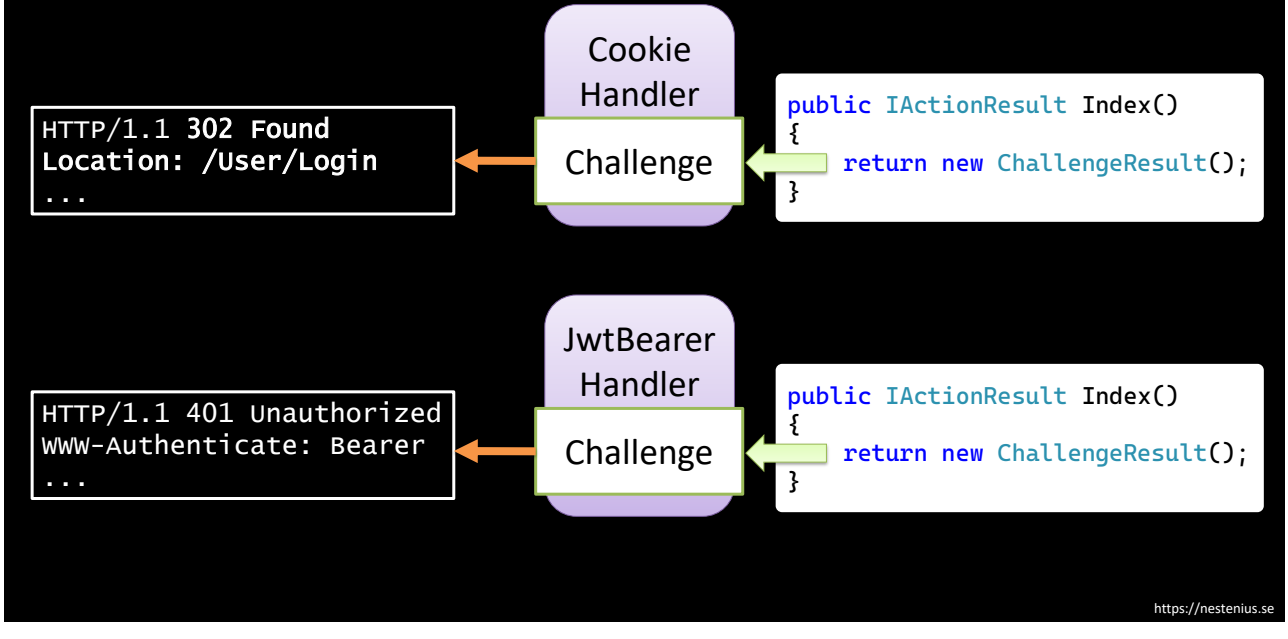


Will challenge always redirect?

https://nestenius.se

31

Challenge != Redirect



https://nestenius.se

32

What is the problem here?

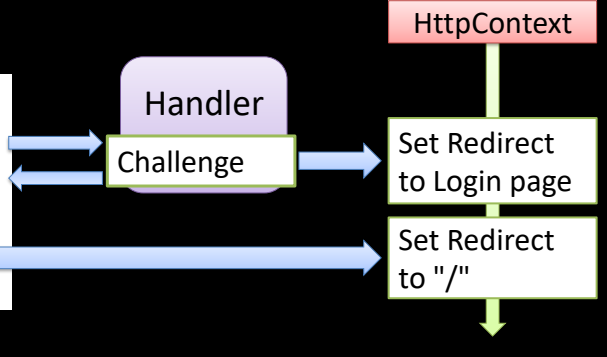
```
public async Task<IActionResult> Index()
{
    await HttpContext.ChallengeAsync();

    return Redirect("/");
}
```

https://nestenius.se

33

Alternatives

```
public async Task<IActionResult> Index()
{
    await HttpContext.ChallengeAsync();


    return Redirect("/");
}
```



https://nestenius.se

34

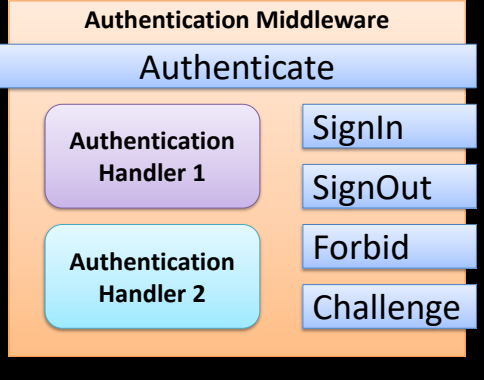
Schemes!

https://nestenius.se

35

Schemes

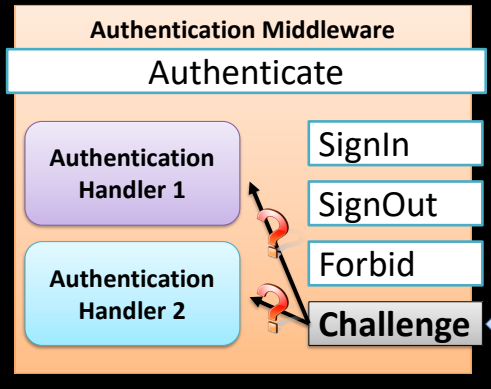
Using Multiple Handlers



https://nestenius.se

36

Schemes



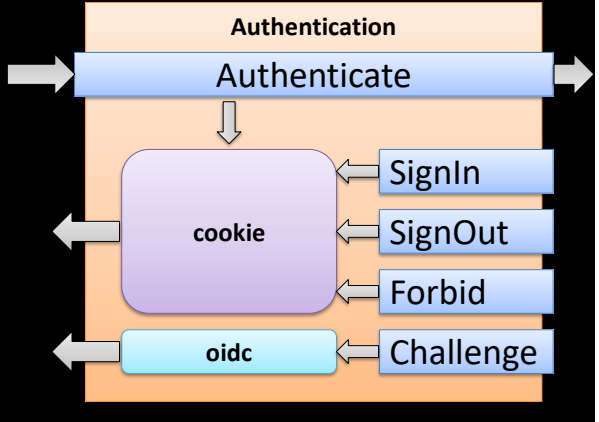

```
public async Task<IActionResult> Index()
{
    if (User.Identity.IsAuthenticated == false)
    {
        return Challenge();
    }

    return View();
}
```

https://nestenius.se

37

Schemes

```
builder.Services.AddAuthentication(o =>
{
    o.DefaultChallengeScheme = "oidc";
    o.DefaultAuthenticateScheme = "cookie";
    o.DefaultForbidScheme = "cookie";
    o.DefaultSignInScheme = "cookie";
    o.DefaultSignOutScheme = "cookie";
})
.AddCookie("cookie", opt =>
{
  ...
})
.AddOpenIdConnect("oidc", opt =>
{
  ...
});
```



https://nestenius.se

38

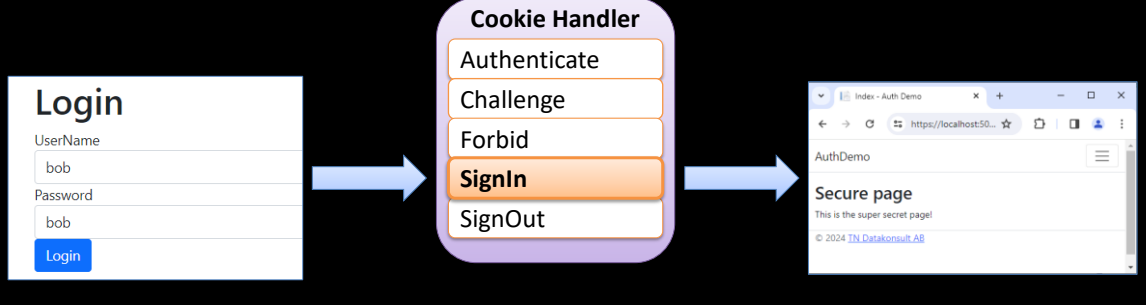
Live coding #4

```
builder.Services.AddAuthentication(o =>
{
    o.DefaultScheme = "cookie";
})
.AddCookie("cookie", o =>
{
    o.LoginPath = "/user/login";
    o.LogoutPath = "/user/loggedOut";
    o.AccessDeniedPath = "/user/AccessDenied";
});
```

https://nestenius.se

39

SignIn the User



https://nestenius.se

40

The Login Action Methods

```
[HttpGet]
public IActionResult Login(string ReturnUrl)
{
    return View(new LoginModel() { ReturnUrl = ReturnUrl });
}

[HttpPost]
[ValidateAntiForgeryToken]
public async Task Login(LoginModel loginCredentials)
{
    //...
}
```

```
public class LoginModel
{
    public string UserName  { get; set; };
    public string Password  { get; set; };
    public string ReturnUrl { get; set; };
}
```

https://nestenius.se

41

Create the list of claims

```
[HttpPost]
[ValidateAntiForgeryToken]
public async Task Login(LoginModel loginCredentials)
{

    //1. Validate username + password

    //2. Load the claims for this user from the DB
    var claims = new List<Claim>()
                 {
                     new("sub","1234"),
                     new("name","Bob"),
                     new("email","bob@tn-data.se"),
                     new("role","developer")
                 };

    //...

}
```

https://nestenius.se

42

Create an Identity + ClaimsPrincipal

```
//1. Validate username + password

//2. Load the claims for this user from the DB
var claims = new List<Claim>()
    {
        new("sub","1234"),
        new("name","Bob"),
        new("email","bob@tn-data.se"),
        new("role","developer")
    };

//3. Create an Identity for these claims
var identity = new ClaimsIdentity(claims: claims,
                                  authenticationType: "pwd",
                                  nameType: "name",
                                  roleType: "role");

//4. Create the principal based on the users Identity
var principal = new ClaimsPrincipal(identity);
```

Auth types
pwd
External
Windows
Jwt
Cookie
api_key
NTLM
Digest
Basic
Negotiate
...

https://nestenius.se

43

SignIn Principal

```
// ...
var principal = new ClaimsPrincipal(identity);

var prop = new AuthenticationProperties()
{
    RedirectUri = loginCredentials.ReturnUrl,
    Items =
    {
        { "IpAddress", "192.168.0.3" },
        { "ComputerName", "MyComputer" },
        { "ApiKey", "Summer2025!!" }
    }
};

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

https://nestenius.se

44

Live coding #5

```
//1. Validate username + password

//2. Load the claims for this user from the DB
var claims = new List<Claim>()
{
    new("sub","1234"),
    new("name","Bob"),
    new("email","bob@tn-data.se"),
    new("role","developer")
};

var identity = new ClaimsIdentity(claims: claims,
                                  authenticationType: "pwd",
                                  nameType: "name",
                                  roleType: "role");

var principal = new ClaimsPrincipal(identity);

var prop = new AuthenticationProperties()
{
    RedirectUri = "/",
    Items =
    {
        { "IpAddress", "192.168.0.3" },
        { "ComputerName", "MyComputer" },
        { "ApiKey", "Summer2025!!" }
    }
};

await HttpContext.SignInAsync(scheme: "cookie",
                              principal: principal,
                              properties: prop);
return LocalRedirect("/");
```

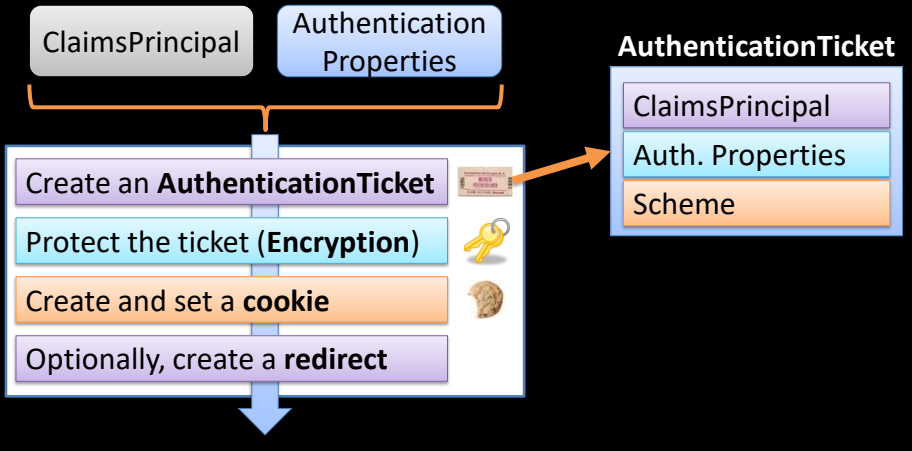
https://nestenius.se

What happens when we call SignInAsync?

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

https://nestenius.se

SignInAsync inside the Cookie Handler



https://nestenius.se

47

What is inside the authentication cookie?

```
Set-Cookie: .AspNetCore.cookie=CfDJ8IgPXRNAZH1EkNA0dd3_JvtpVOohM43sH8lB8MW4
2T1L57tPORRWmJu8svjUYUwIrYUOW4xoOikClOR3H87teUK4MYy58NBBAsjc8RDRWhKO6JVzOHuHW1eNSfu
nLJ_OOObZ1y6kYlF52lkzI8cw8VLPzG4zm33hoynL2JHLTCoWbugN-3kyOLrUSyVJdotB1ANGcvBT-
jz2rAFuOeUbzCdXXDjm98YzW3E99QffLamD1LlrKe7MX1y31NWdxzQ39m4WmGwUNa3bOiHoyDaeSKJvifmz
lMSWT_8o9x4AUtzC6_whIOfPVHXhYkwCXGTwtpIYeb_KOGuAvidb3S3tTkK4m3LHcf5Fx9ajfbE8RC_5FLO
sPxbQiQcF3KGmIUPOdnHmtK7MHczg4UR-OgBh_TA_sKyMoPy9Ak9sa4P-XvMWWyssEkOOzxfHbi6F
VWbq5CNDe6W1QZG6z5PwtwGsVmx4vK8C3_4b9r-HU; path=/; secure; samesite=lax; httponly
```

https://nestenius.se

48

Live coding #6

```
.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

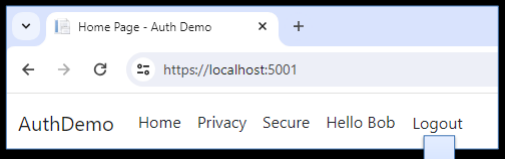
49

SignOut

https://nestenius.se

50

SignOut




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

Cookie Handler

- Authenticate
- Challenge
- Forbid
- SignIn
- **SignOut**

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

https://nestenius.se

51

Live coding #7

```
[HttpPost]
public async Task Logout()
{
    await HttpContext.SignOutAsync("cookie");
}
```

https://nestenius.se

52

Redirect After SignOut

https://nestenius.se

53

LogoutPath

```
builder.Services.AddAuthentication()
                .AddCookie(o =>
                {
                    ...
                    o.LogoutPath = "/user/LoggedOut";
                });
```

```
await HttpContext.SignOutAsync("cookie");
```

```
HTTP/1.1 200 OK
Content-Length: 0
Set-Cookie: .AspNetCore.cookie=; expires=Thu, 01 Jan 1970 00:00:00 GMT;...
```

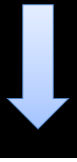
Why are we not redirected?

https://nestenius.se

54

Live coding #8

```
<form action="/User/Logout" method="post">
  <button type="submit">Logout</button>
</form>
```



```
<form action="/User/Logout?ReturnUrl=/User/LoggedOut" method="post">
  <button type="submit">Logout</button>
</form>
```

https://nestenius.se

55

Using ReturnUrl

/User/Logout?ReturnUrl=/User/LoggedOut

```
builder.Services.AddAuthentication()
                .AddCookie(o =>
                {
                    ...
                    o.LogoutPath = "/user/LoggedOut";
                    ...
                });
```

```
HTTP/1.1 200 OK
Content-Length: 0
Set-Cookie: .AspNetCore.cookie=; expires=Thu, 01 Jan 1970 00:00:00 GMT;...
```

https://nestenius.se

56

Live coding #9

/User/Logout?ReturnUrl=/User/LoggedOut

```
.AddCookie(o =>
{
   ...
  o.LogoutPath = "/user/LoggedOut";
   ...
});
```

```
.AddCookie(o =>
{
   ...
   o.LogoutPath = "/user/LogOut";
   ...
});
```

```
HTTP/1.1 302 Found
Location: /User/LoggedOut
Set-Cookie: .AspNetCore.cookie=; expires=Thu, 01 Jan 1970 00:00:00 GMT;...
```

https://nestenius.se

57

Alternatives

```
[HttpPost]
public async Task Logout()
{
    var properties = new AuthenticationProperties()
    {
        RedirectUri = "/User/LoggedOut"
    };

    await HttpContext.SignOutAsync("cookie", properties);
}
```

```
[HttpPost]
public async Task<IActionResult> Logout()
{
    await HttpContext.SignOutAsync("cookie");

    return LocalRedirect("/User/LoggedOut");
}
```

https://nestenius.se

58

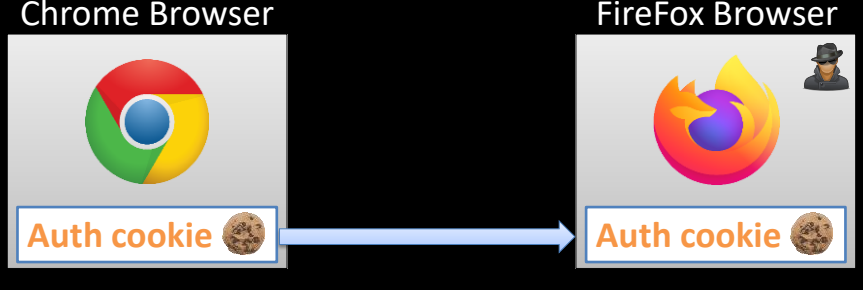
Are we really signed out?

```
[HttpPost]
public async Task Logout()
{
    await HttpContext.SignOutAsync("cookie");
}
```

https://nestenius.se

59

Live coding #10



https://nestenius.se

60

Live coding #11

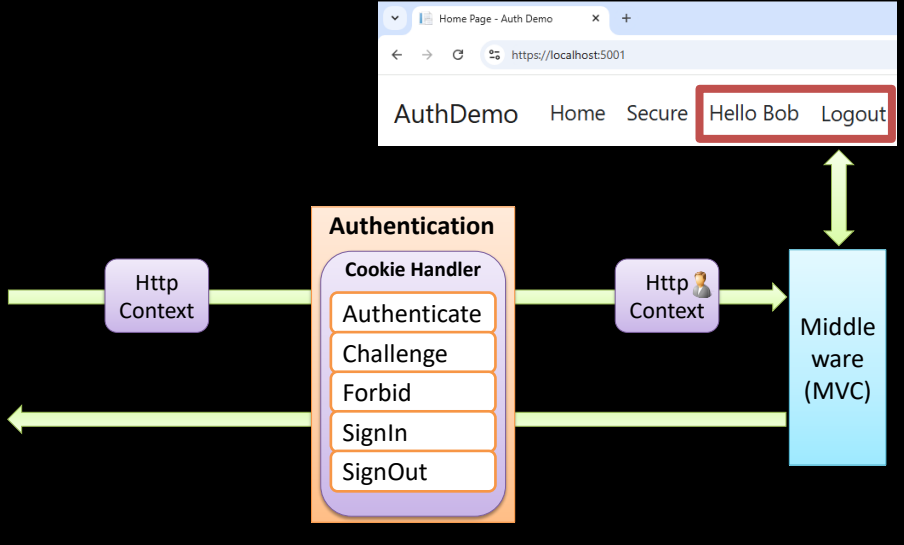
Large cookies!

```
var claims = new List<Claim>()
{
    new("sub","1234" + new string('x',10000)),
    new("name","Bob"),
    new("email","bob@tn-data.se"),
    new("role","developer")
};
```

https://nestenius.se

61

Summary



https://nestenius.se

62

The End

QUESTIONS?

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

Blog
nestenius.se

Work
tn-data.se

https://nestenius.se