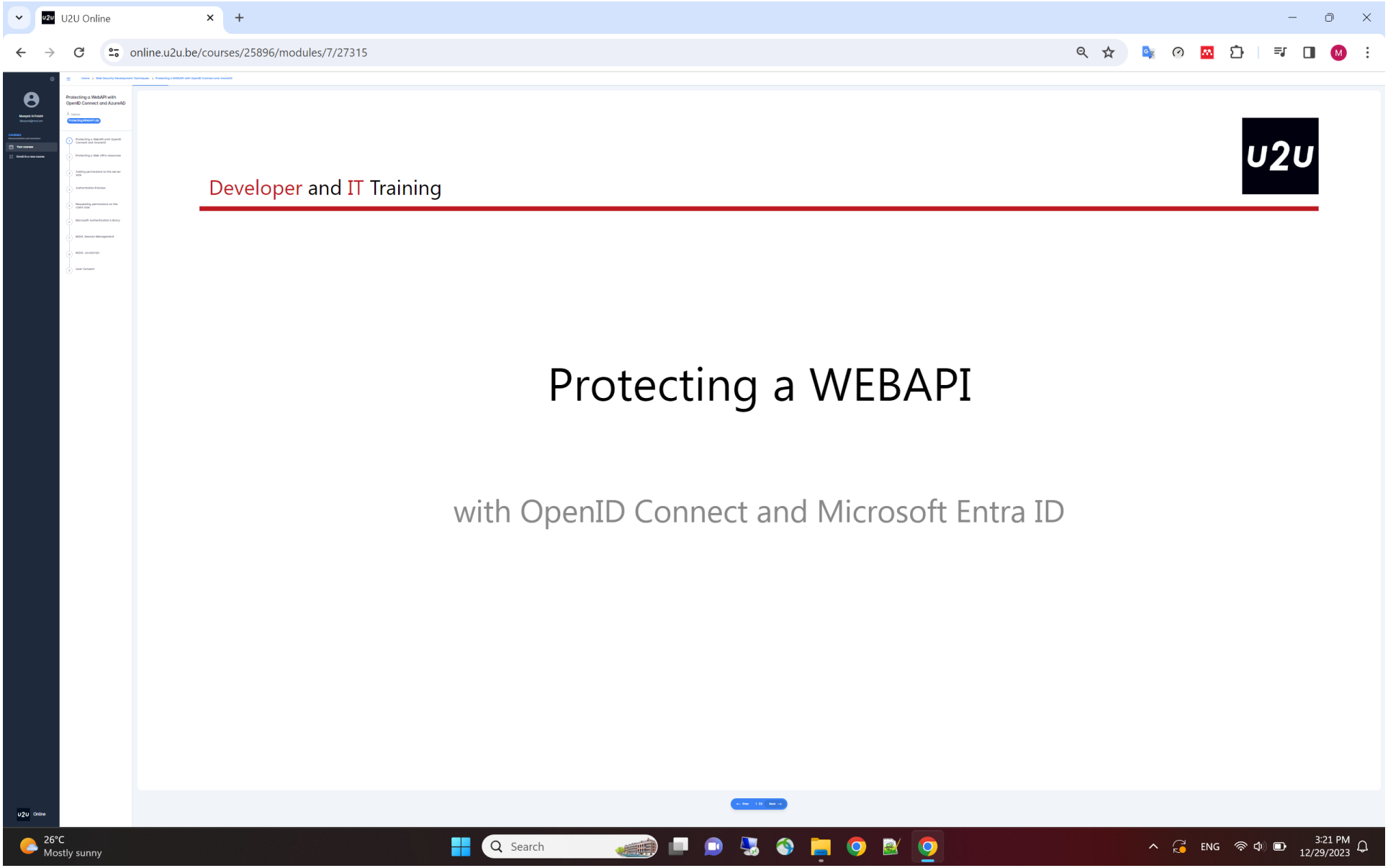
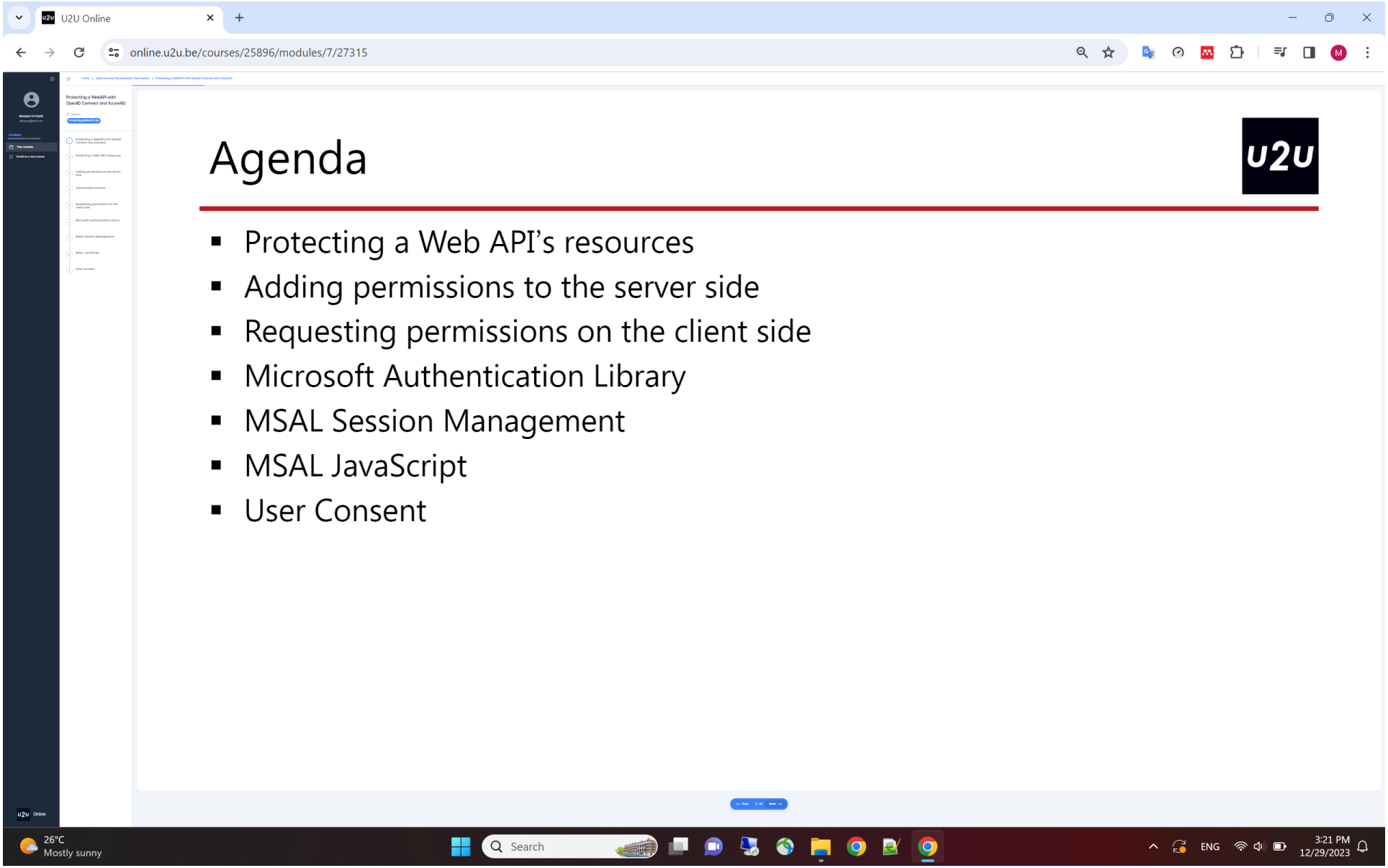
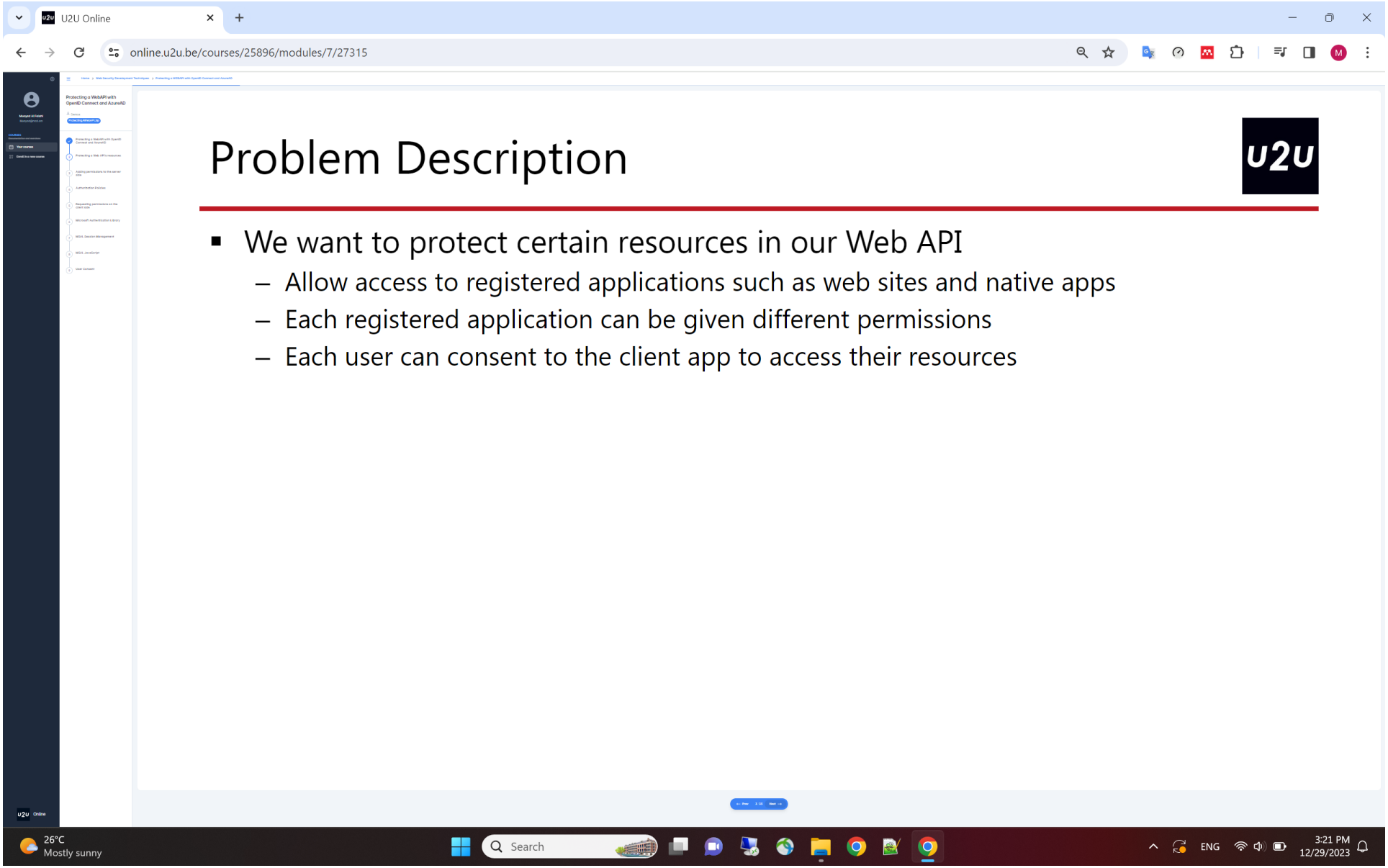
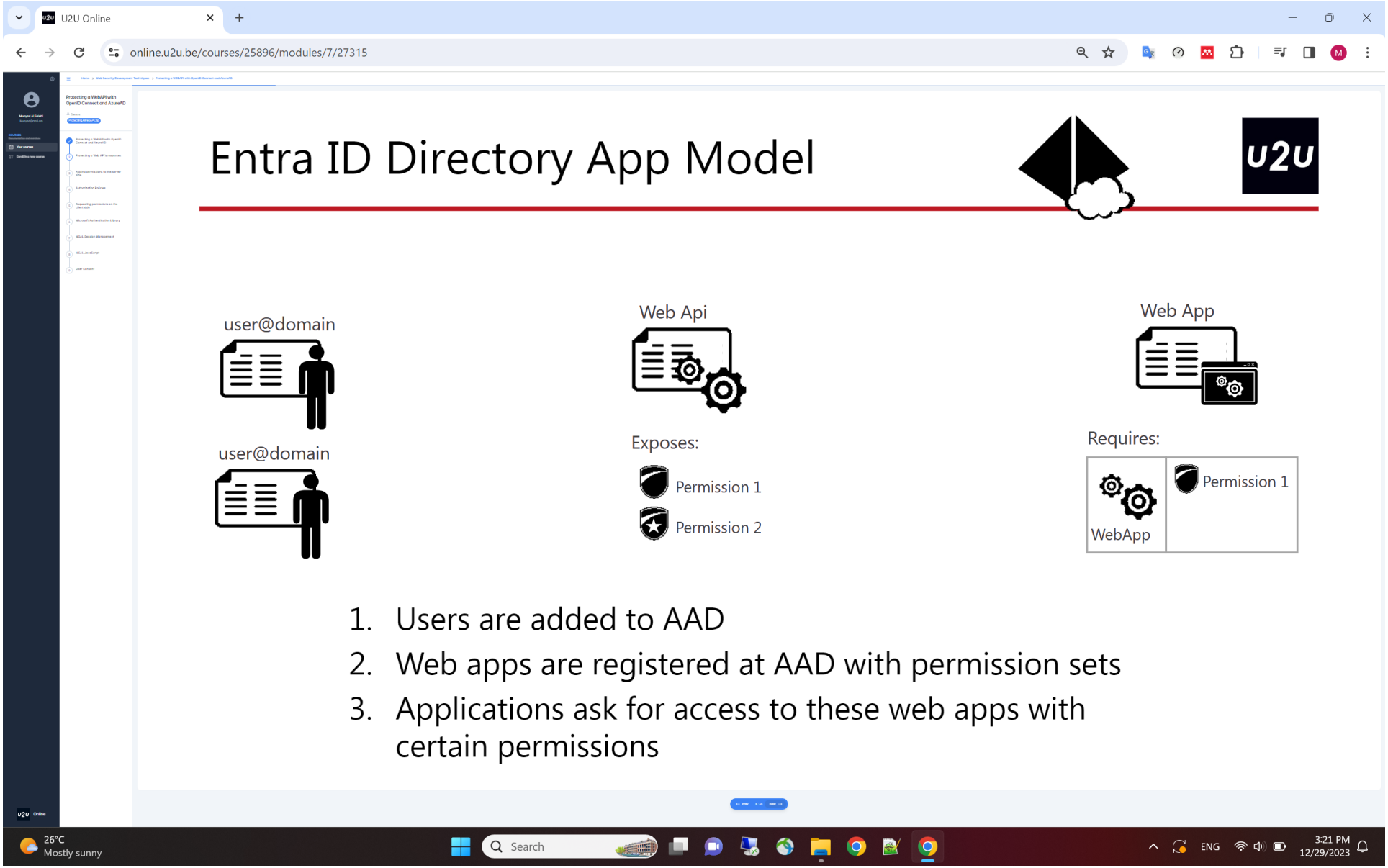
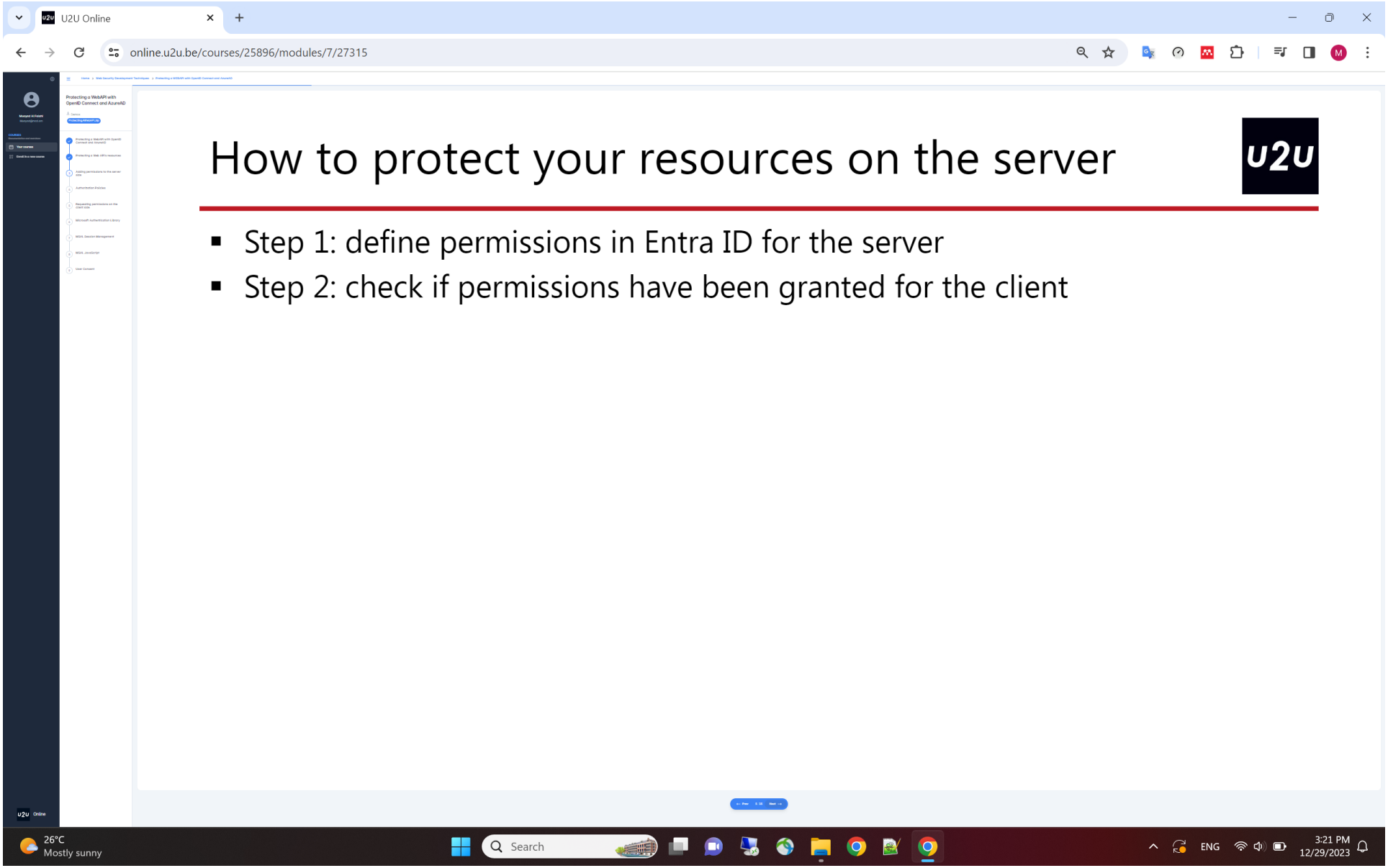

U2U Online
online.u2u.be/courses/25896/modules/7/27315
Developer and IT Training
U2U
Protecting a WEBAPI
with OpenID Connect and Microsoft Entra ID
26°C
Mostly sunny
Search
ENG
3:21 PM
12/29/2023


U2U Online
online.u2u.be/courses/25896/modules/7/27315
Agenda
U2U
Protecting a Web API's resources
Adding permissions to the server side
Requesting permissions on the client side
Microsoft Authentication Library
MSAL Session Management
MSAL JavaScript
User Consent
26°C
Mostly sunny
Search
ENG
3:21 PM
12/29/2023

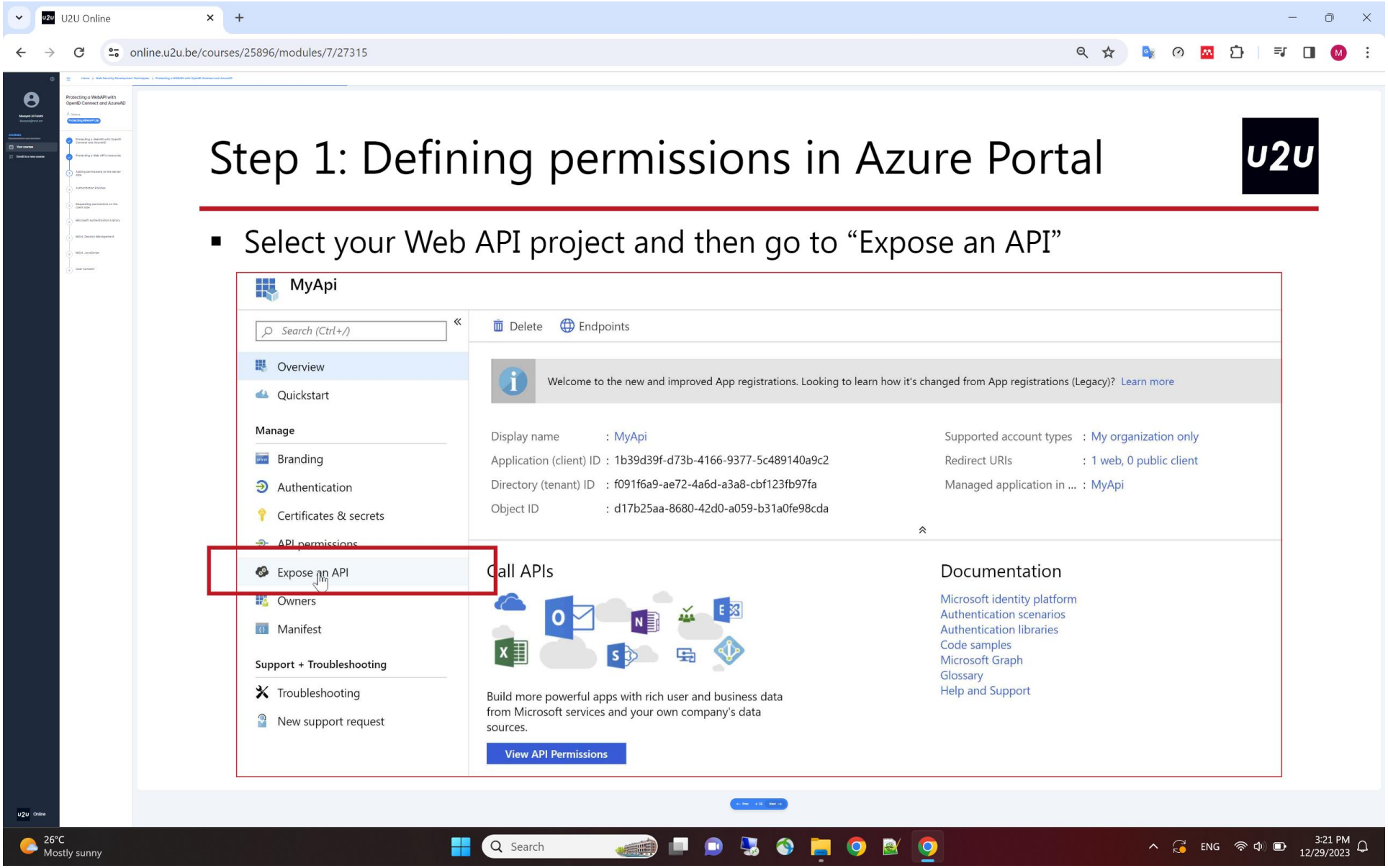

U2U Online
online.u2u.be/courses/25896/modules/7/27315
Problem Description
U2U
We want to protect certain resources in our Web API
Allow access to registered applications such as web sites and native apps
Each registered application can be given different permissions
Each user can consent to the client app to access their resources
26°C
Mostly sunny
Search
ENG
3:21 PM
12/29/2023

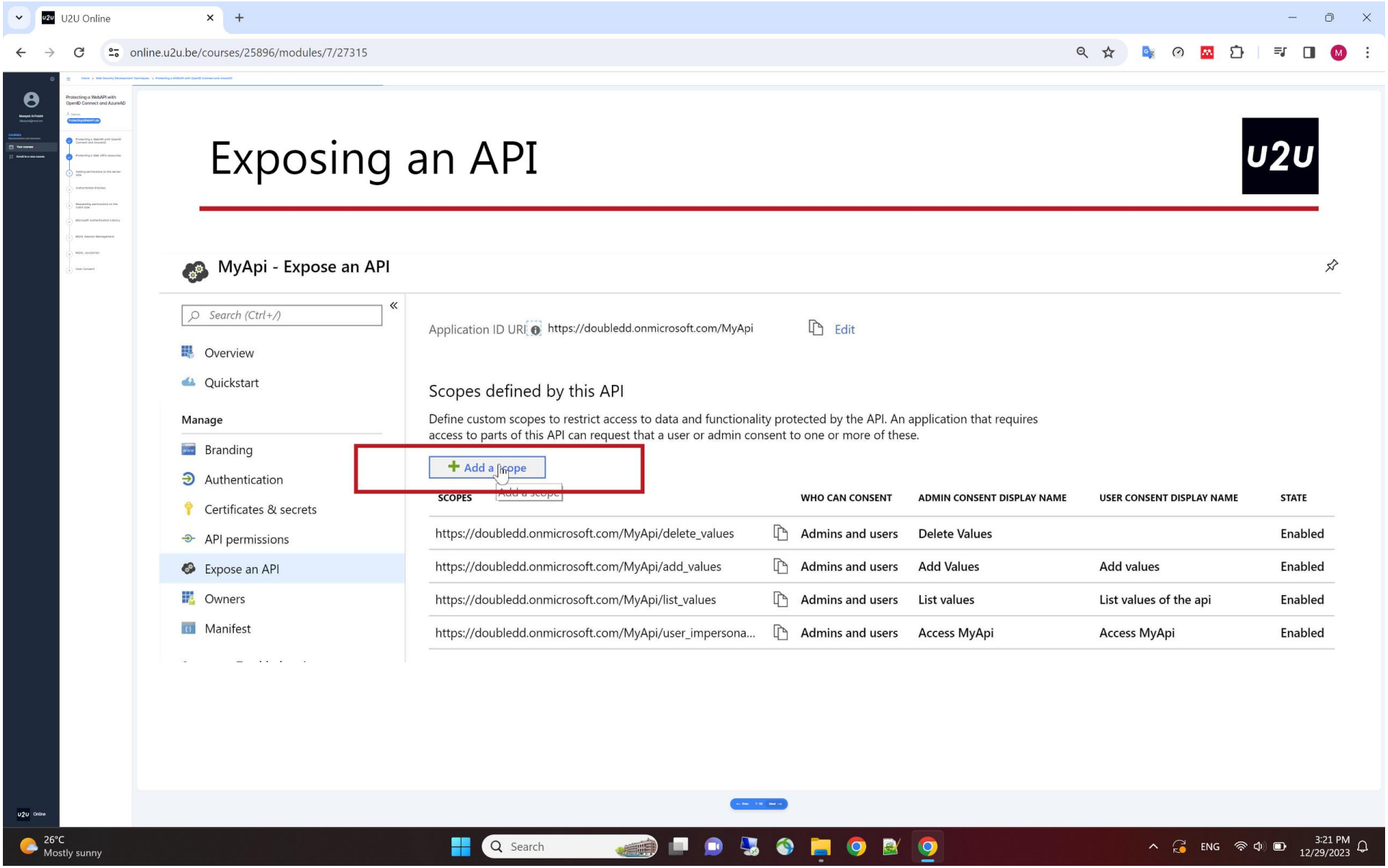

U2U Online
online.u2u.be/courses/25896/modules/7/27315
Entra ID Directory App Model
U2U
user@domain
user@domain
Web Api
Exposes:
Permission 1
Permission 2
Web App
Requires:
WebApp
Permission 1
1. Users are added to AAD
2. Web apps are registered at AAD with permission sets
3. Applications ask for access to these web apps with certain permissions
26°C
Mostly sunny
Search
ENG
3:21 PM
12/29/2023

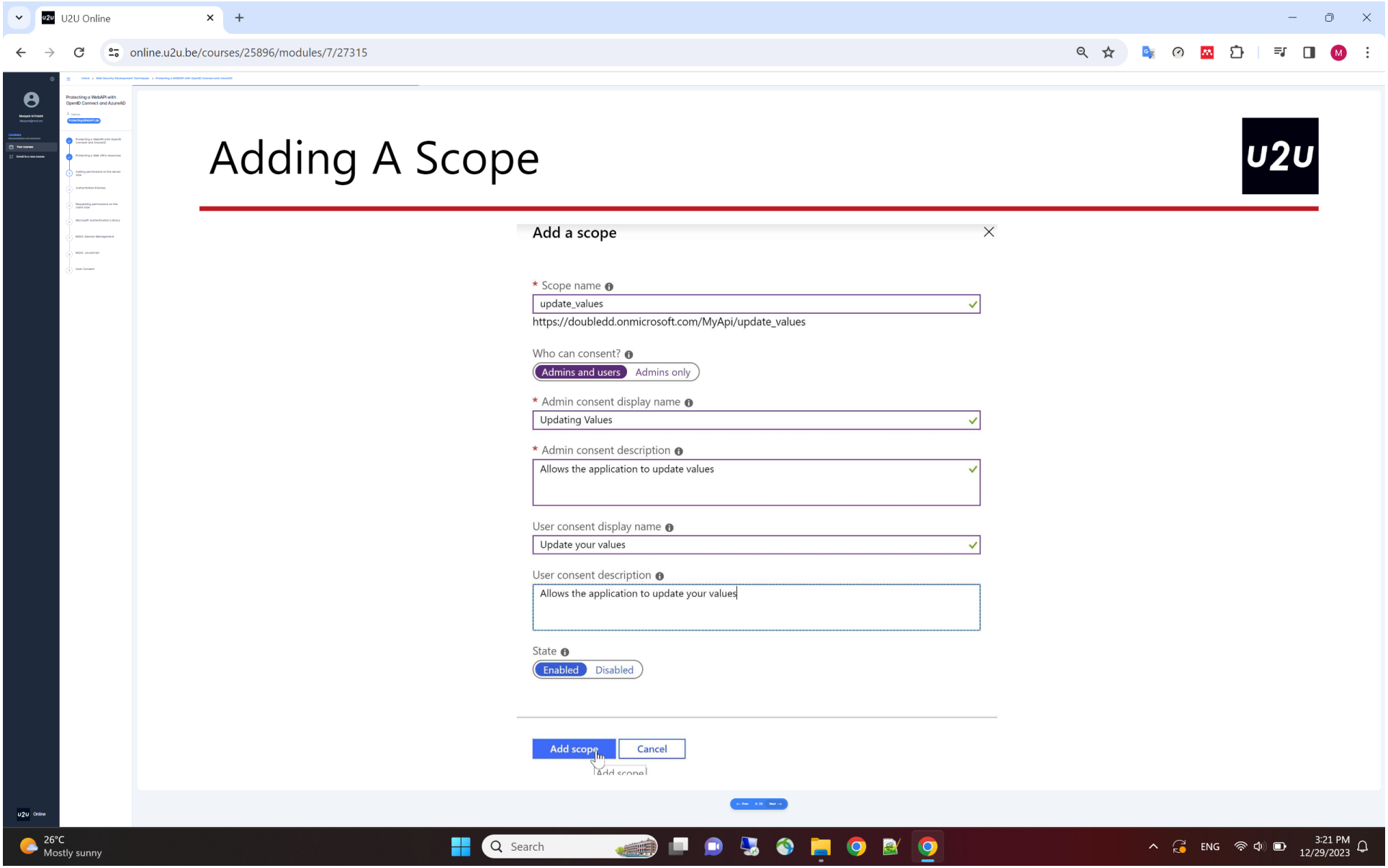

U2U Online
online.u2u.be/courses/25896/modules/7/27315
How to protect your resources on the server
U2U
Step 1: define permissions in Entra ID for the server
Step 2: check if permissions have been granted for the client
26°C
Mostly sunny
Search
ENG
3:21 PM
12/29/2023

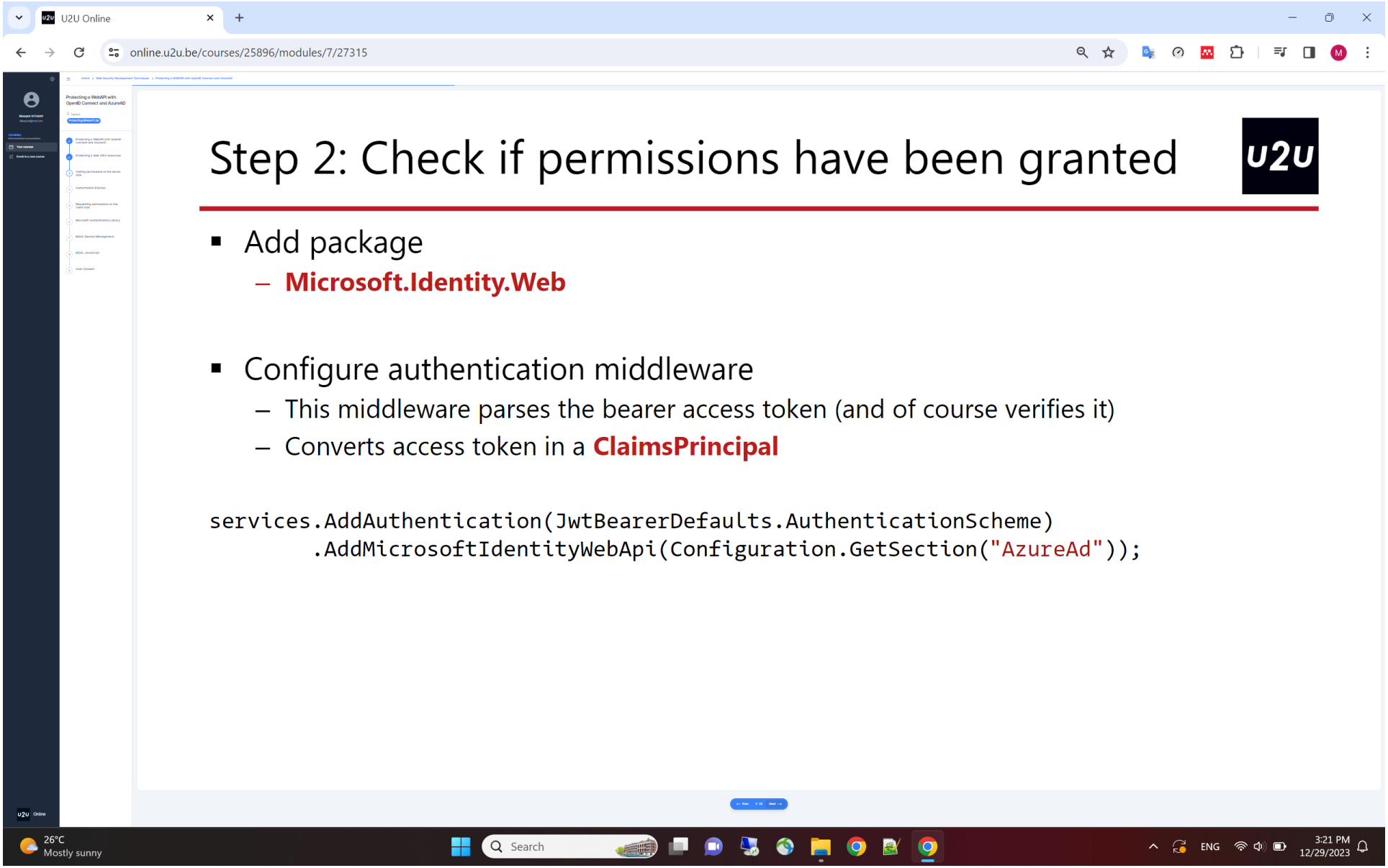
Step 1: Defining permissions in Azure Portal

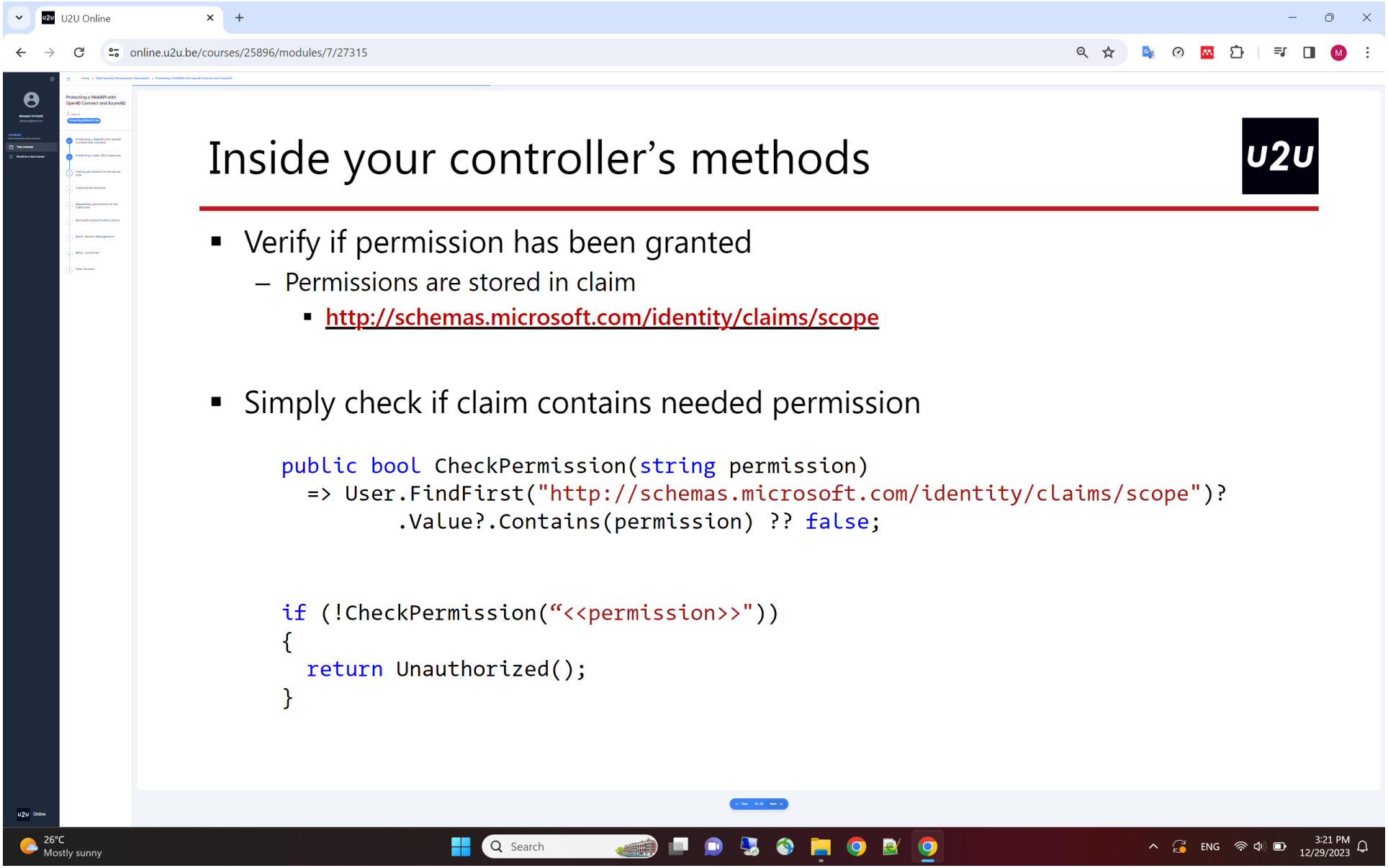
- Select your Web API project and then go to “Expose an API”

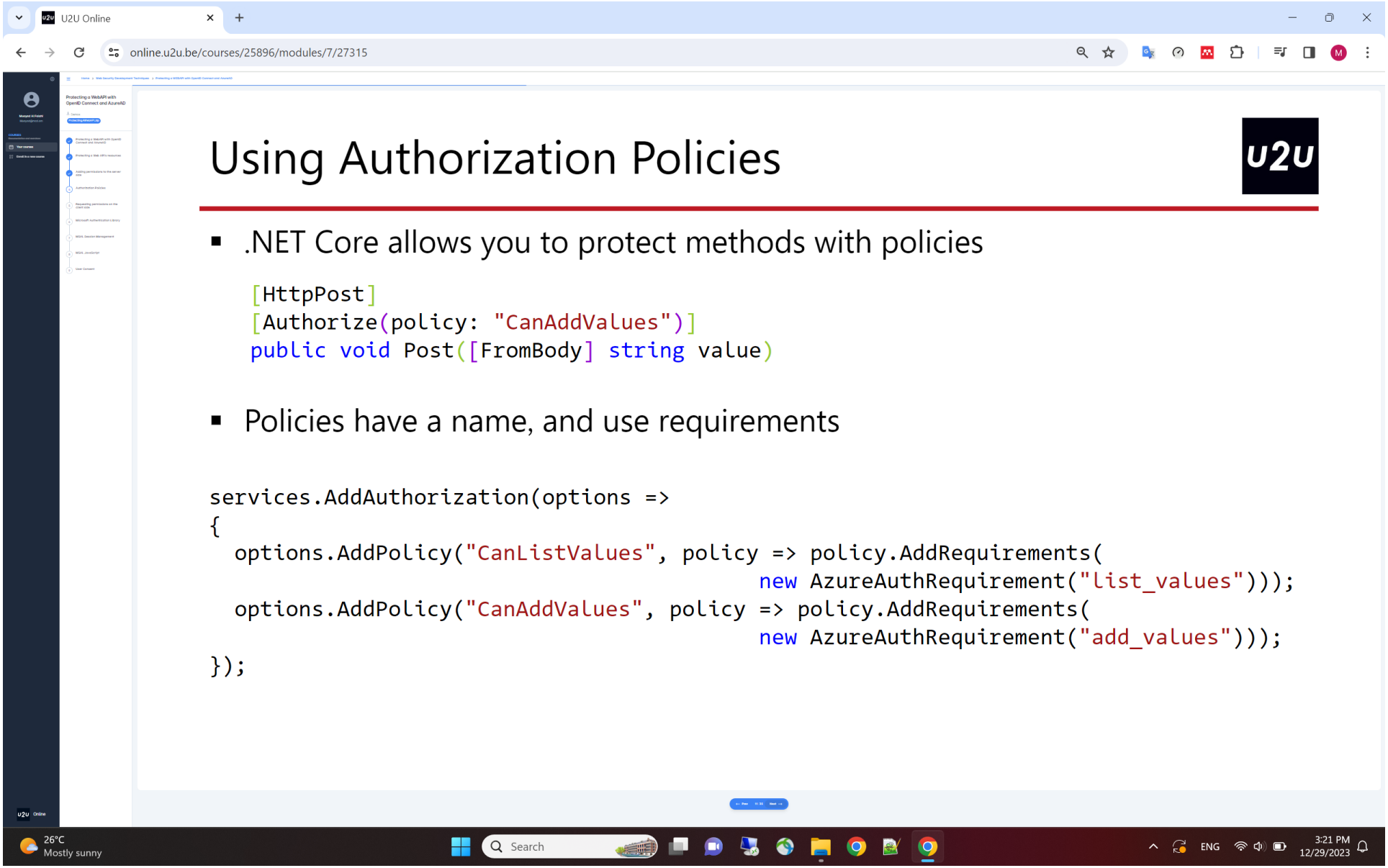


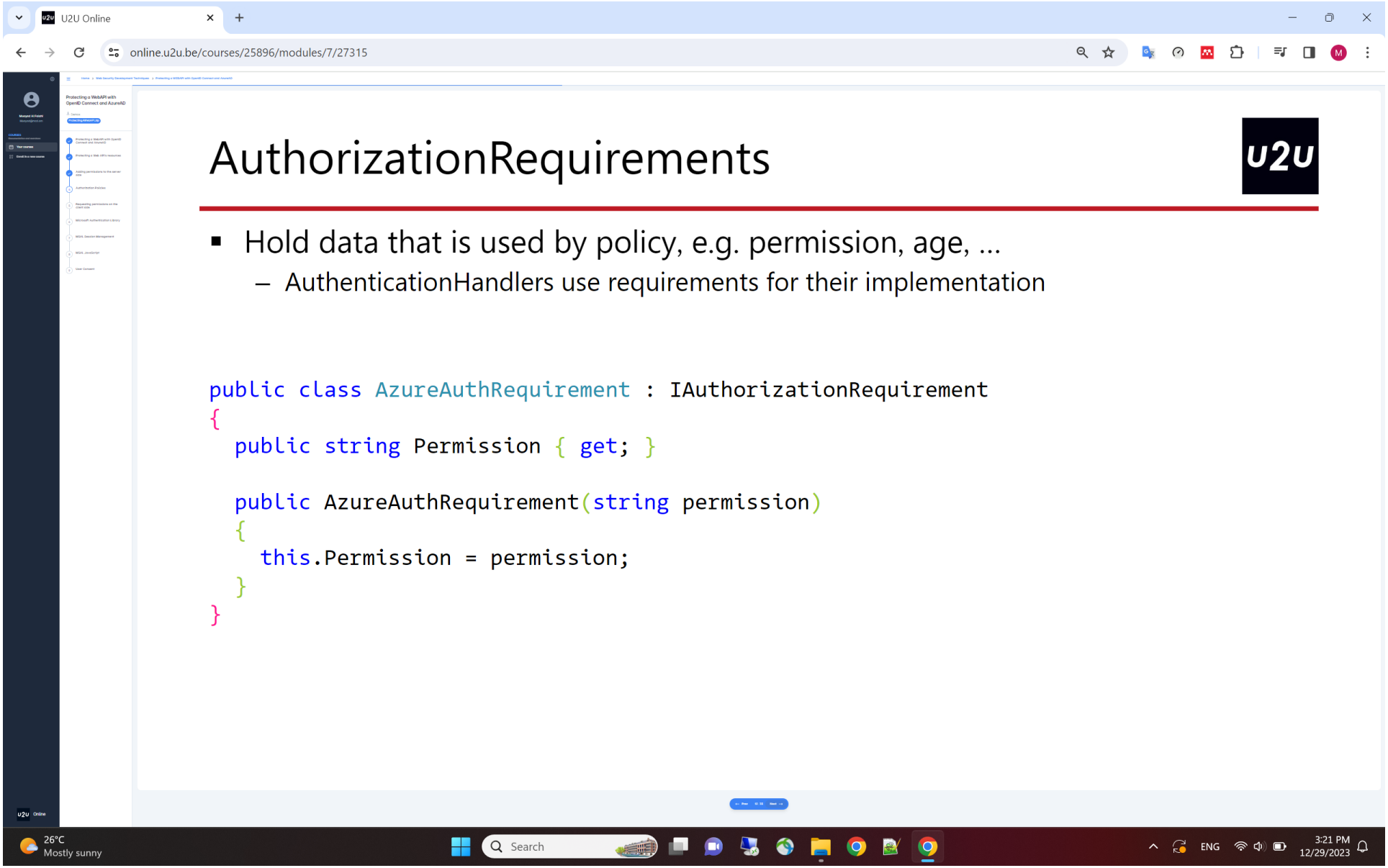

U2U Online
online.u2u.be/courses/25896/modules/7/27315
Exposing an API
U2U
MyApi - Expose an API
Search (Ctrl+/)
Overview
Quickstart
Manage
Branding
Authentication
Certificates & secrets
API permissions
Expose an API
Owners
Manifest
Application ID URI https://doubledd.onmicrosoft.com/MyApi
Edit
Scopes defined by this API
Define custom scopes to restrict access to data and functionality protected by the API. An application that requires access to parts of this API can request that a user or admin consent to one or more of these.
Add a scope
SCOPES
WHO CAN CONSENT
ADMIN CONSENT DISPLAY NAME
USER CONSENT DISPLAY NAME
STATE
https://doubledd.onmicrosoft.com/MyApi/delete_values
Admins and users
Delete Values
Enabled
https://doubledd.onmicrosoft.com/MyApi/add_values
Admins and users
Add Values
Add values
Enabled
https://doubledd.onmicrosoft.com/MyApi/list_values
Admins and users
List values
List values of the api
Enabled
https://doubledd.onmicrosoft.com/MyApi/user_impersona...
Admins and users
Access MyApi
Access MyApi
Enabled
26°C
Mostly sunny
Search
ENG
3:21 PM
12/29/2023

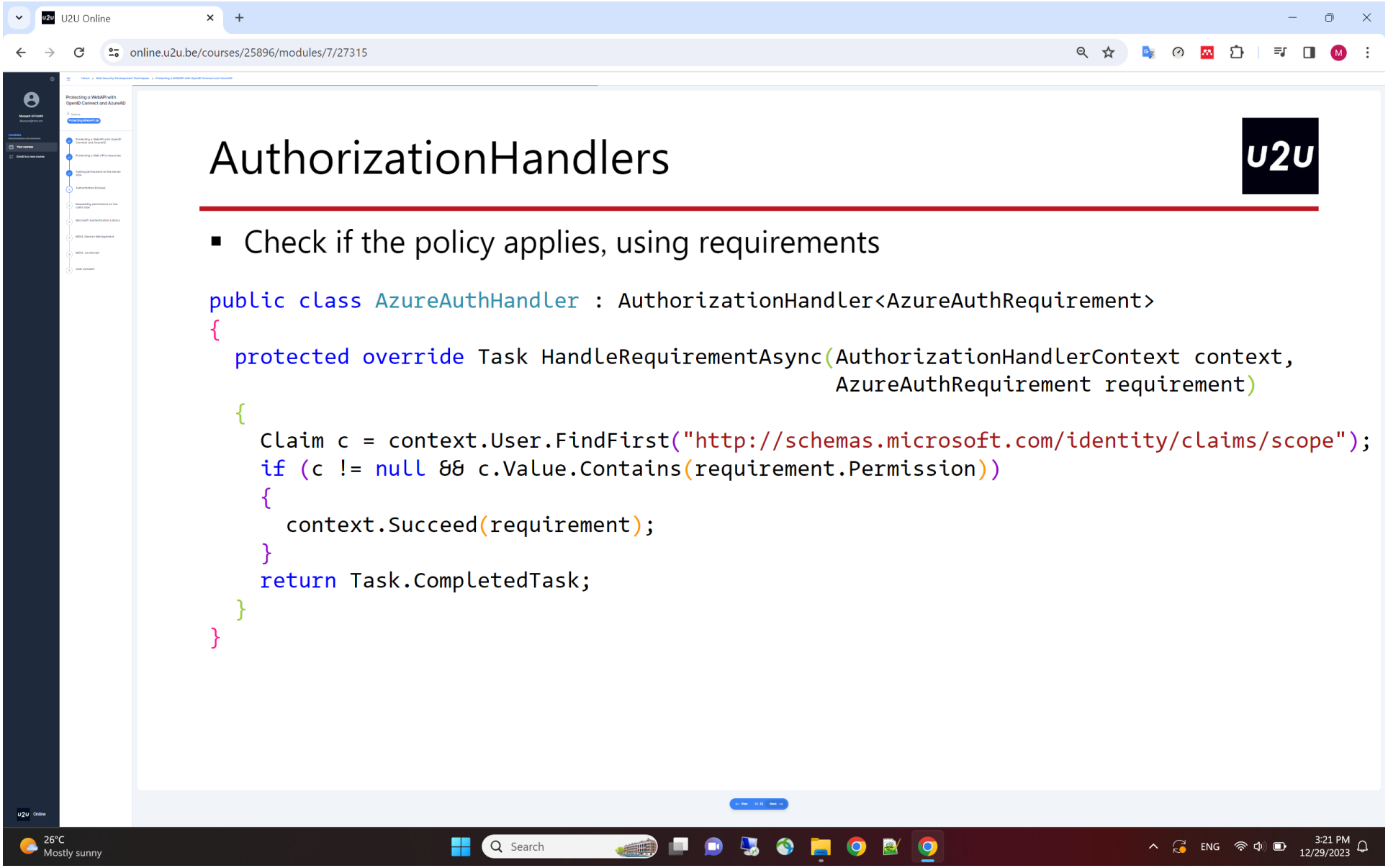

U2U Online
online.u2u.be/courses/25896/modules/7/27315
Adding A Scope
u2u
Add a scope
* Scope name
update_values
https://doubledd.onmicrosoft.com/MyApi/update_values
Who can consent?
Admins and users
Admins only
* Admin consent display name
Updating Values
* Admin consent description
Allows the application to update values
User consent display name
Update your values
User consent description
Allows the application to update your values
State
Enabled
Disabled
Add scope
Cancel
26°C
Mostly sunny
Search
ENG
3:21 PM
12/29/2023

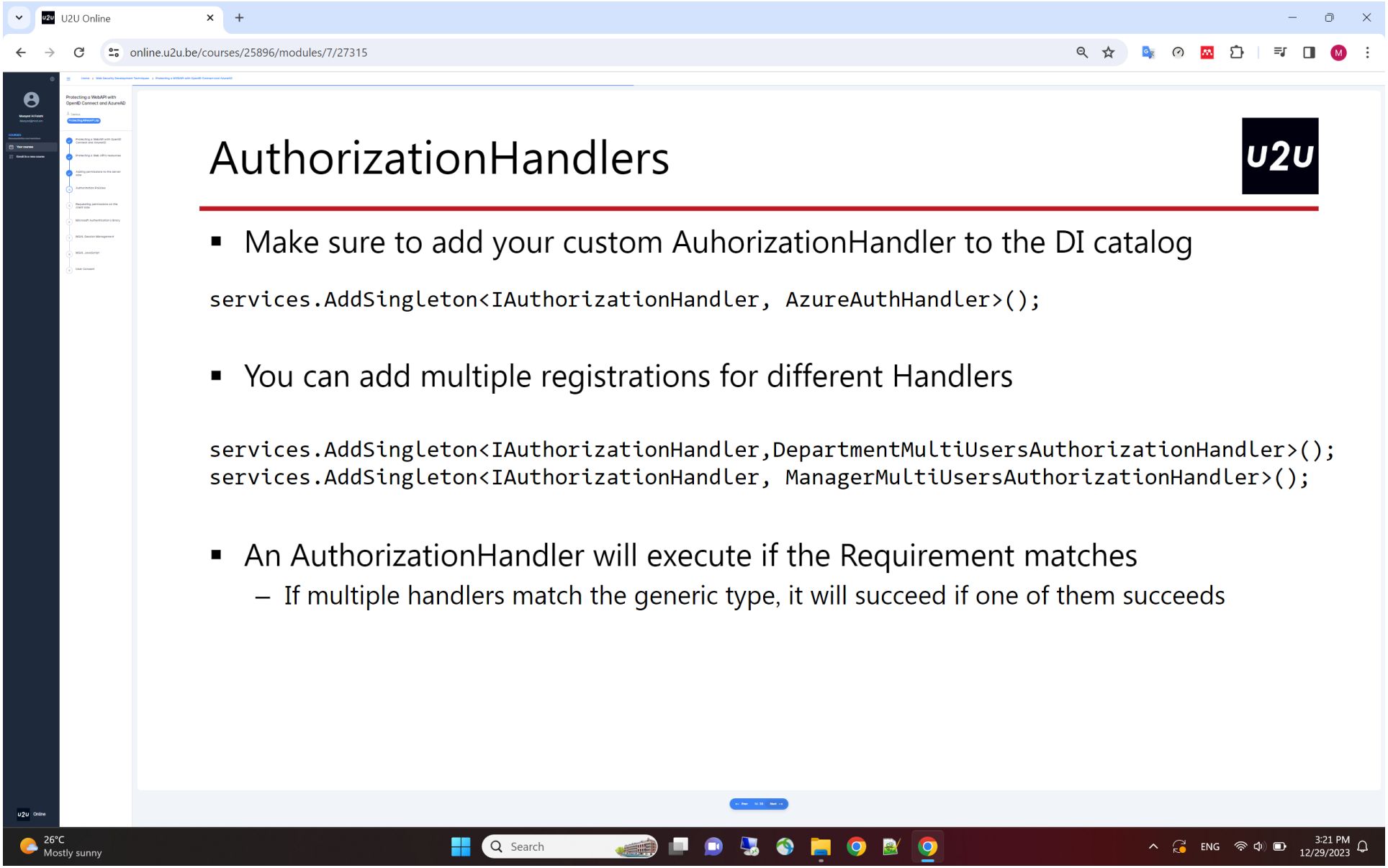

U2U Online
online.u2u.be/courses/25896/modules/7/27315
Step 2: Check if permissions have been granted
u2u
Add package
Microsoft.Identity.Web
Configure authentication middleware
This middleware parses the bearer access token (and of course verifies it)
Converts access token in a ClaimsPrincipal
services.AddAuthentication(JwtBearerDefaults.AuthenticationScheme)
.AddMicrosoftIdentityWebApi(Configuration.GetSection("AzureAd"));
26°C
Mostly sunny
Search
ENG
3:21 PM
12/29/2023

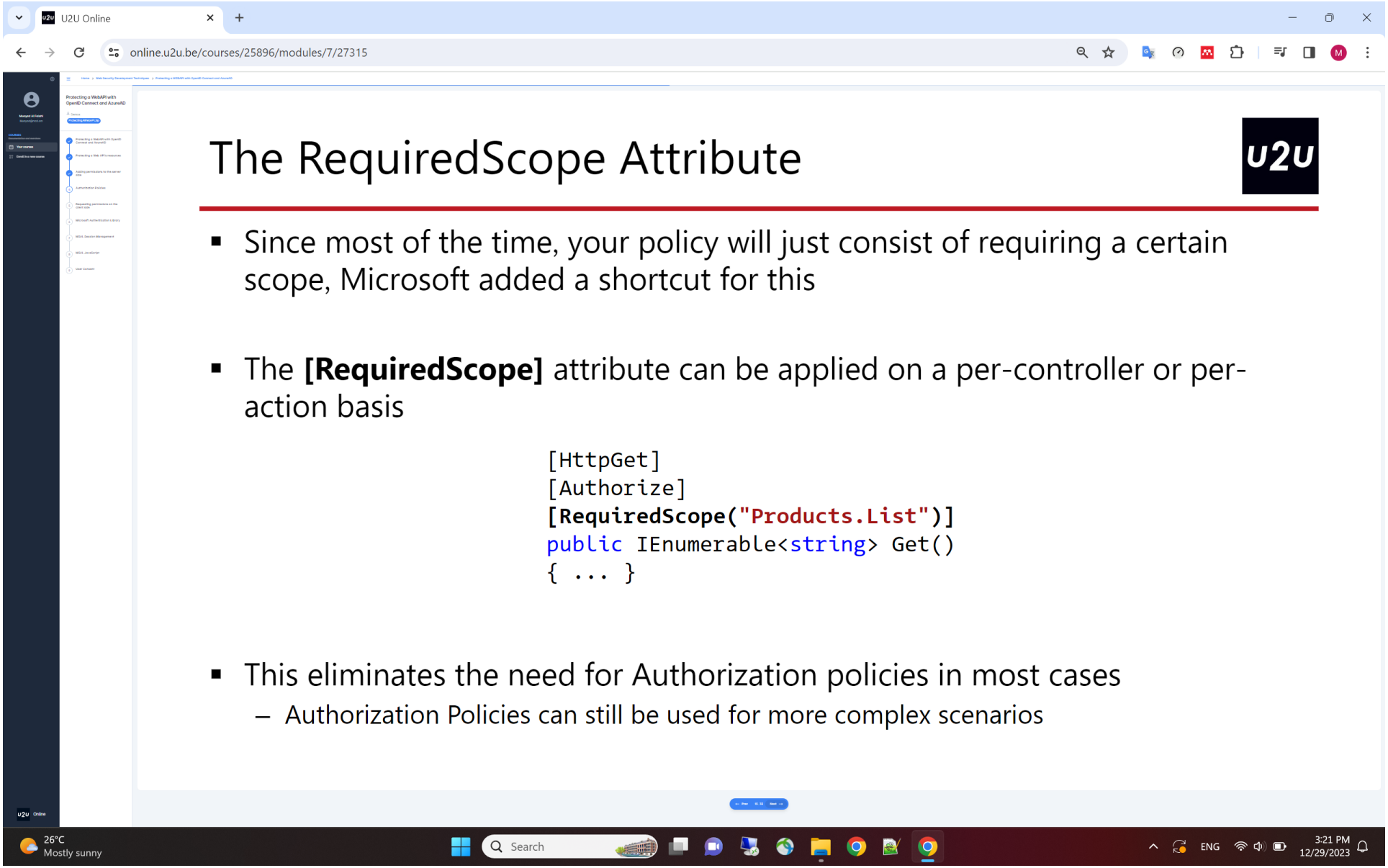

U2U Online
online.u2u.be/courses/25896/modules/7/27315
Inside your controller's methods
U2U
Verify if permission has been granted
Permissions are stored in claim
http://schemas.microsoft.com/identity/claims/scope
Simply check if claim contains needed permission
public bool CheckPermission(string permission)
=> User.FindFirst("http://schemas.microsoft.com/identity/claims/scope")?
.Value?.Contains(permission) ?? false;
if (!CheckPermission("<<permission>>"))
{
return Unauthorized();
}
26°C
Mostly sunny
Search
ENG
3:21 PM
12/29/2023

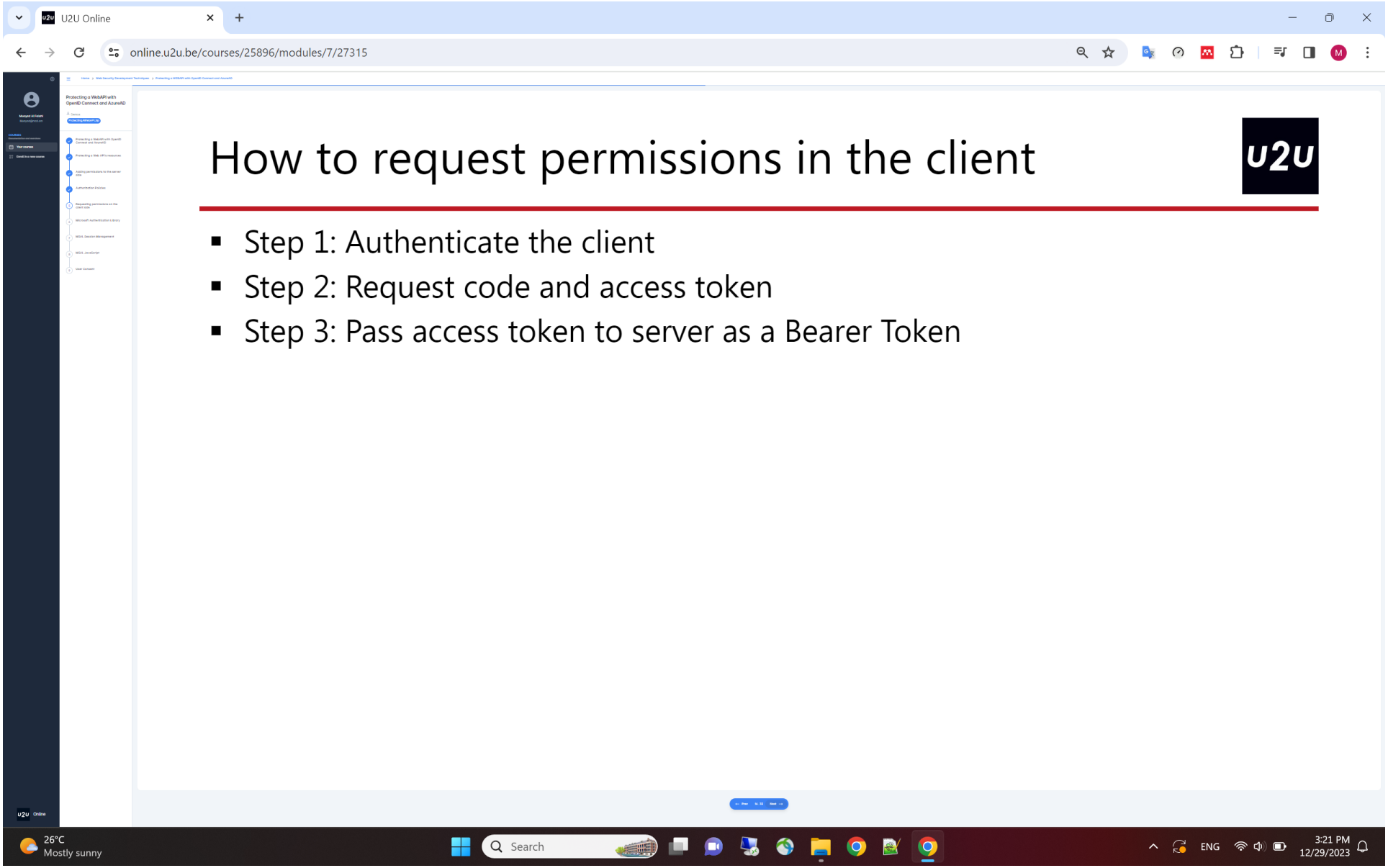

U2U Online
online.u2u.be/courses/25896/modules/7/27315
Using Authorization Policies
U2U
.NET Core allows you to protect methods with policies
[HttpPost]
[Authorize(policy: "CanAddValues")]
public void Post([FromBody] string value)
Policies have a name, and use requirements
services.AddAuthorization(options =>
{
options.AddPolicy("CanListValues", policy => policy.AddRequirements(
new AzureAuthRequirement("list_values")));
options.AddPolicy("CanAddValues", policy => policy.AddRequirements(
new AzureAuthRequirement("add_values")));
});
26°C
Mostly sunny
Search
ENG
3:21 PM
12/29/2023

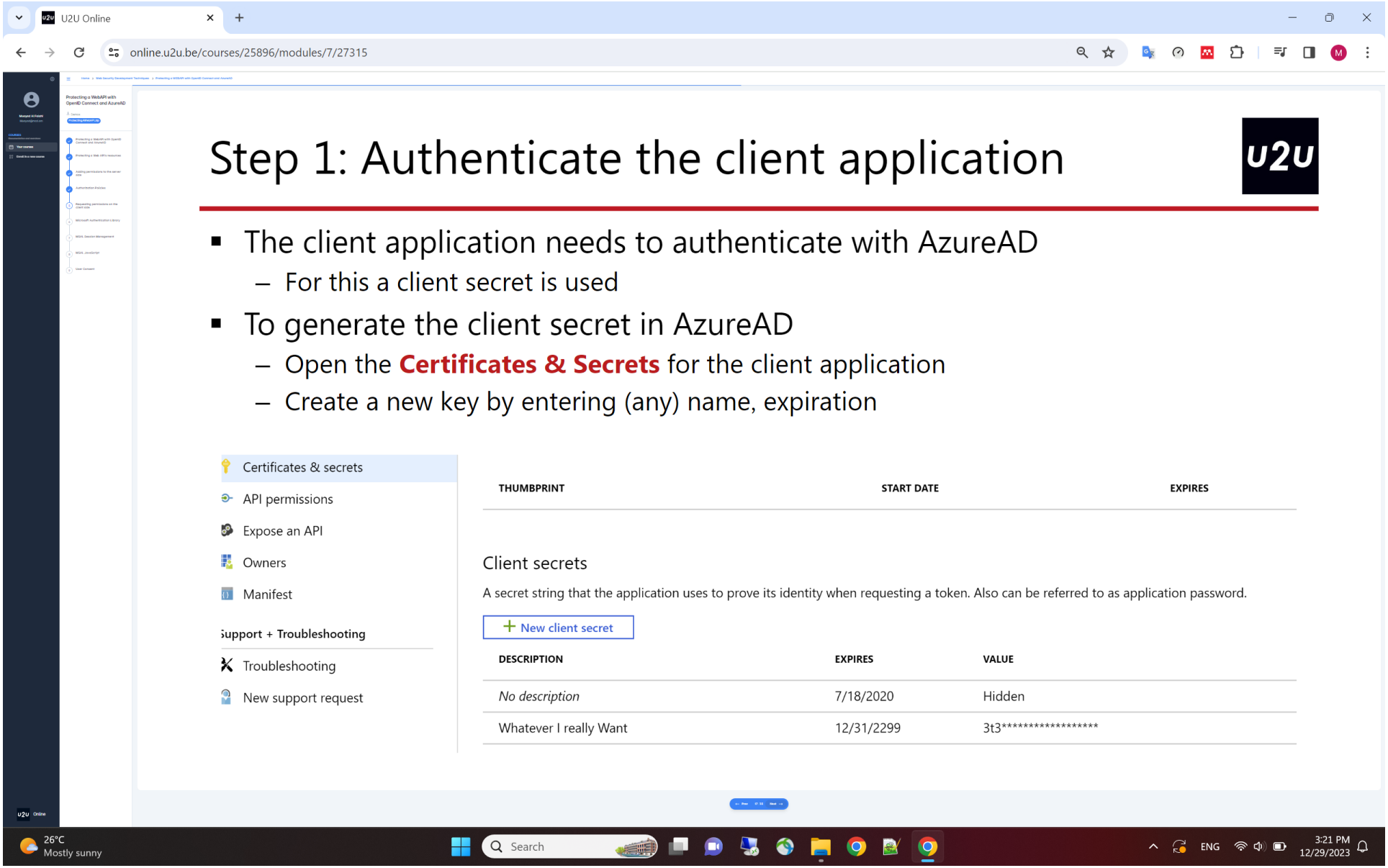

U2U Online
online.u2u.be/courses/25896/modules/7/27315
AuthorizationRequirements
U2U
Hold data that is used by policy, e.g. permission, age, ...
AuthenticationHandlers use requirements for their implementation
public class AzureAuthRequirement : IAuthorizationRequirement
{
public string Permission { get; }
public AzureAuthRequirement(string permission)
{
this.Permission = permission;
}
}
26°C
Mostly sunny
Search
ENG
3:21 PM
12/29/2023

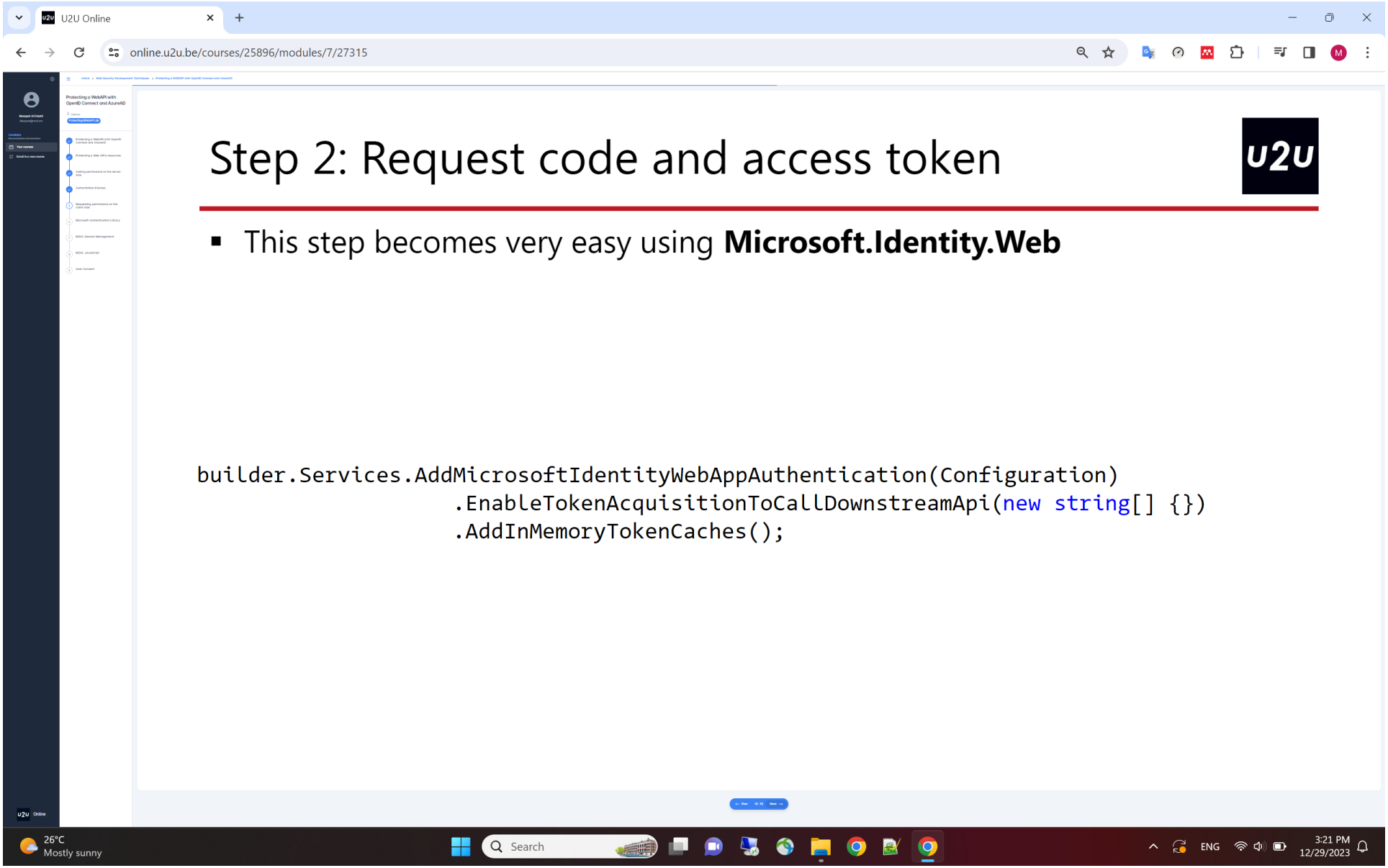

U2U Online
online.u2u.be/courses/25896/modules/7/27315
AuthorizationHandlers
U2U
Check if the policy applies, using requirements
public class AzureAuthHandler : AuthorizationHandler<AzureAuthRequirement>
{
protected override Task HandleRequirementAsync(AuthorizationHandlerContext context,
AzureAuthRequirement requirement)
{
Claim c = context.User.FindFirst("http://schemas.microsoft.com/identity/claims/scope");
if (c != null && c.Value.Contains(requirement.Permission))
{
context.Succeed(requirement);
}
return Task.CompletedTask;
}
}
26°C
Mostly sunny
Search
ENG
3:21 PM
12/29/2023

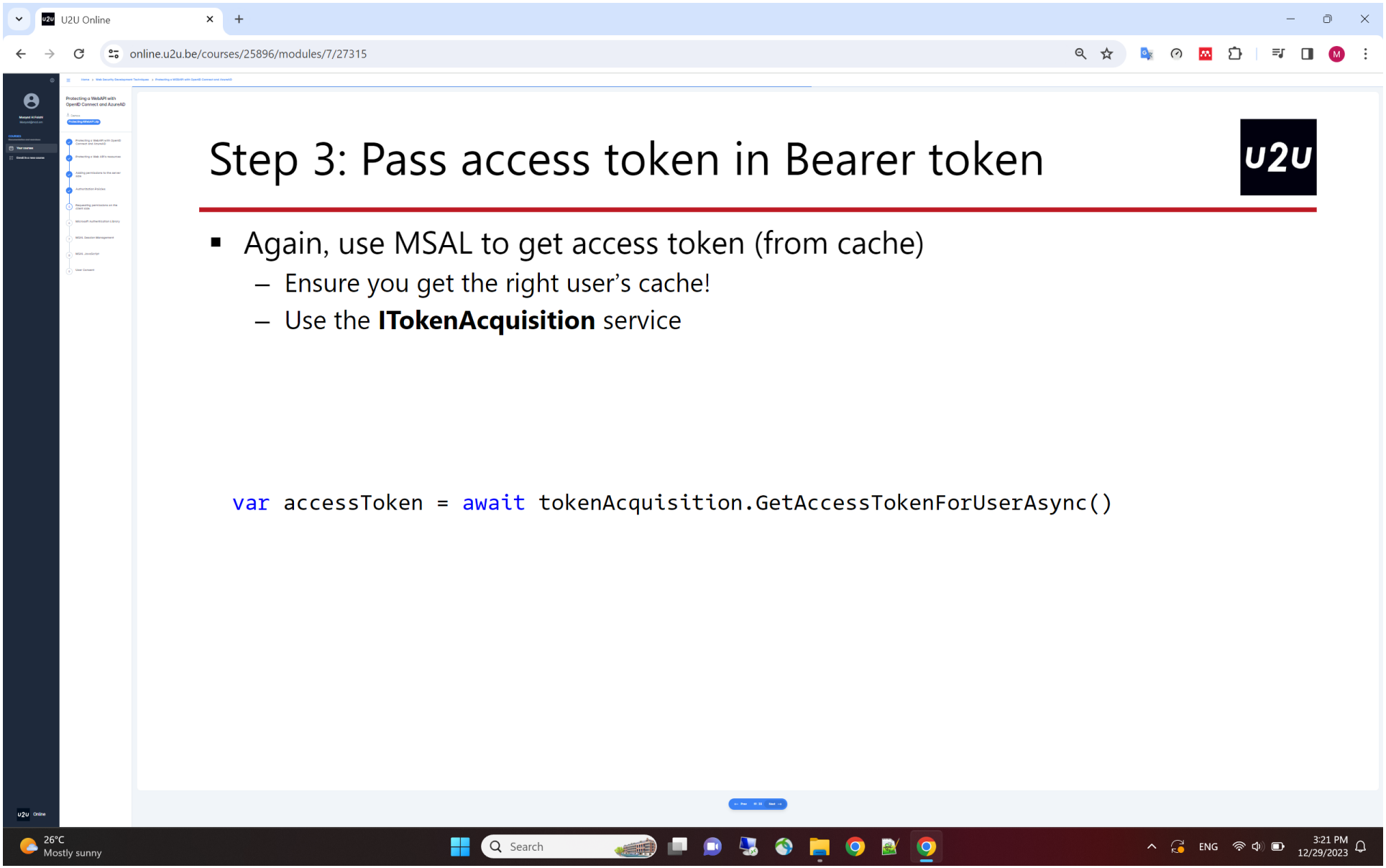

U2U Online
online.u2u.be/courses/25896/modules/7/27315
AuthorizationHandlers
U2U
Make sure to add your custom AuhorizationHandler to the DI catalog
services.AddSingleton<IAuthorizationHandler, AzureAuthHandler>();
You can add multiple registrations for different Handlers
services.AddSingleton<IAuthorizationHandler,DepartmentMultiUsersAuthorizationHandler>();
services.AddSingleton<IAuthorizationHandler, ManagerMultiUsersAuthorizationHandler>();
An AuthorizationHandler will execute if the Requirement matches
If multiple handlers match the generic type, it will succeed if one of them succeeds
26°C
Mostly sunny
Search
ENG
3:21 PM
12/29/2023

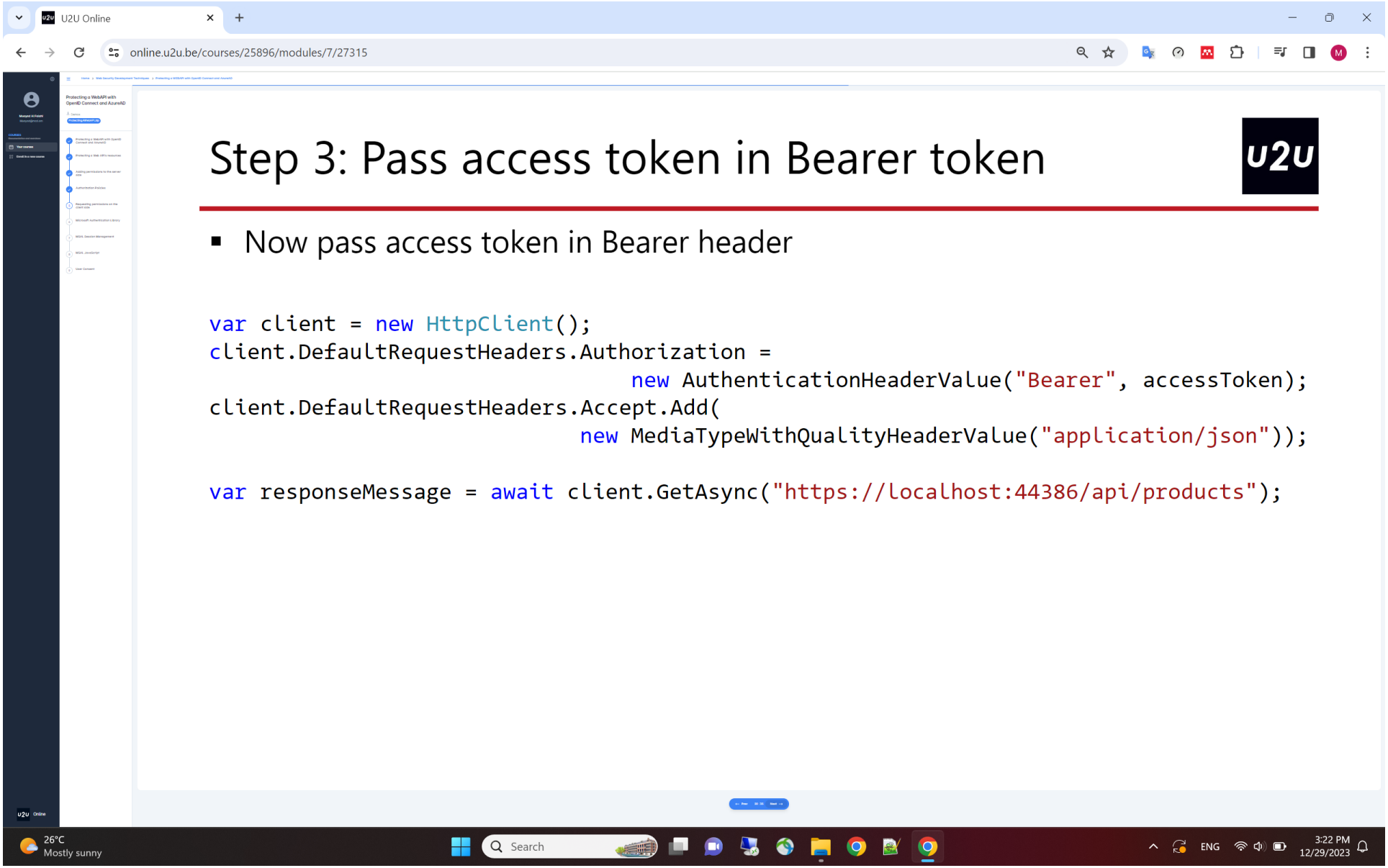

U2U Online
online.u2u.be/courses/25896/modules/7/27315
The RequiredScope Attribute
U2U
Since most of the time, your policy will just consist of requiring a certain scope, Microsoft added a shortcut for this
The [RequiredScope] attribute can be applied on a per-controller or per-action basis
[HttpGet]
[Authorize]
[RequiredScope("Products.List")]
public IEnumerable<string> Get()
{ ... }
This eliminates the need for Authorization policies in most cases
Authorization Policies can still be used for more complex scenarios
26°C
Mostly sunny
Search
ENG
3:21 PM
12/29/2023

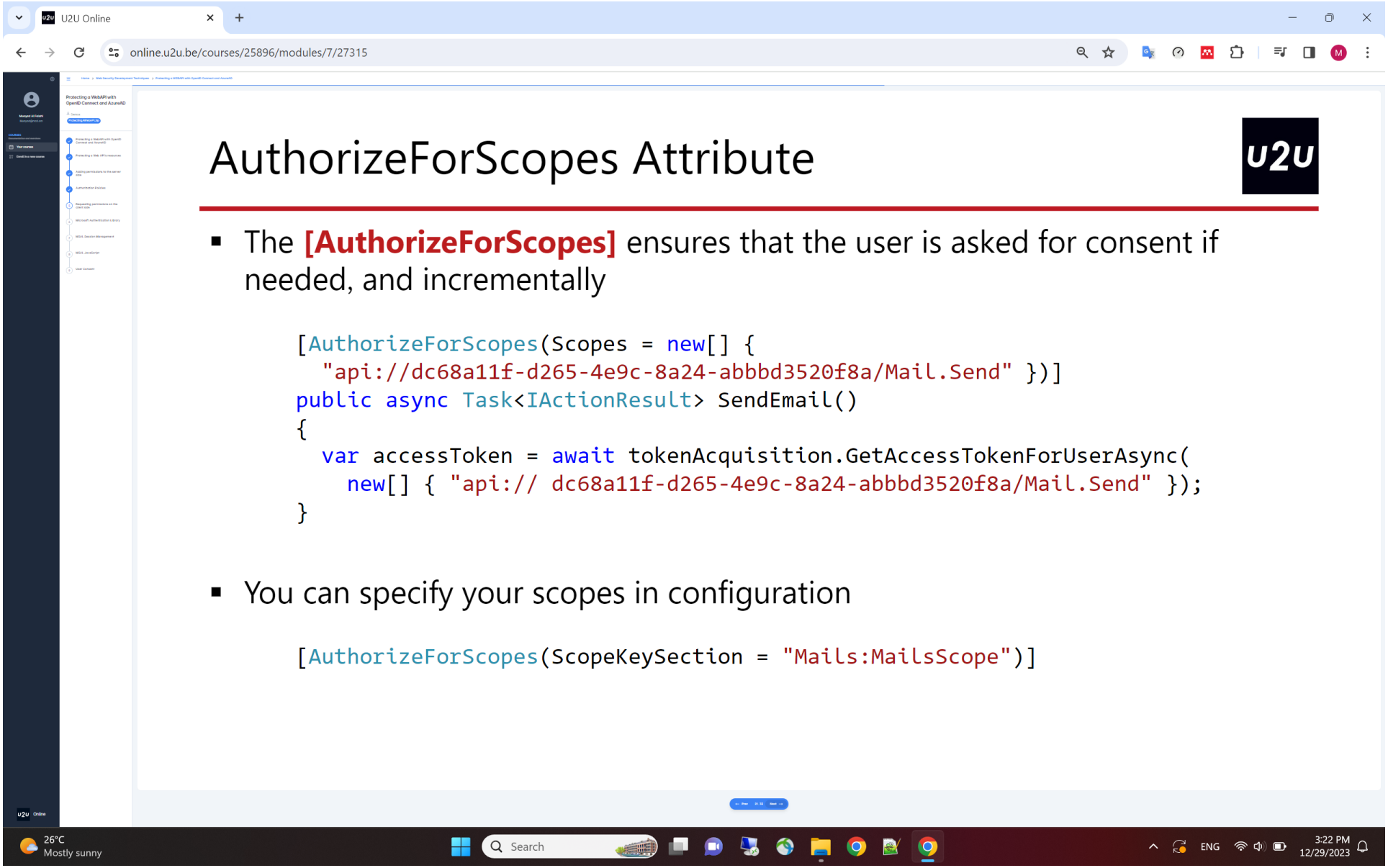

U2U Online
online.u2u.be/courses/25896/modules/7/27315
How to request permissions in the client
U2U
Step 1: Authenticate the client
Step 2: Request code and access token
Step 3: Pass access token to server as a Bearer Token
26°C
Mostly sunny
Search
ENG
3:21 PM
12/29/2023

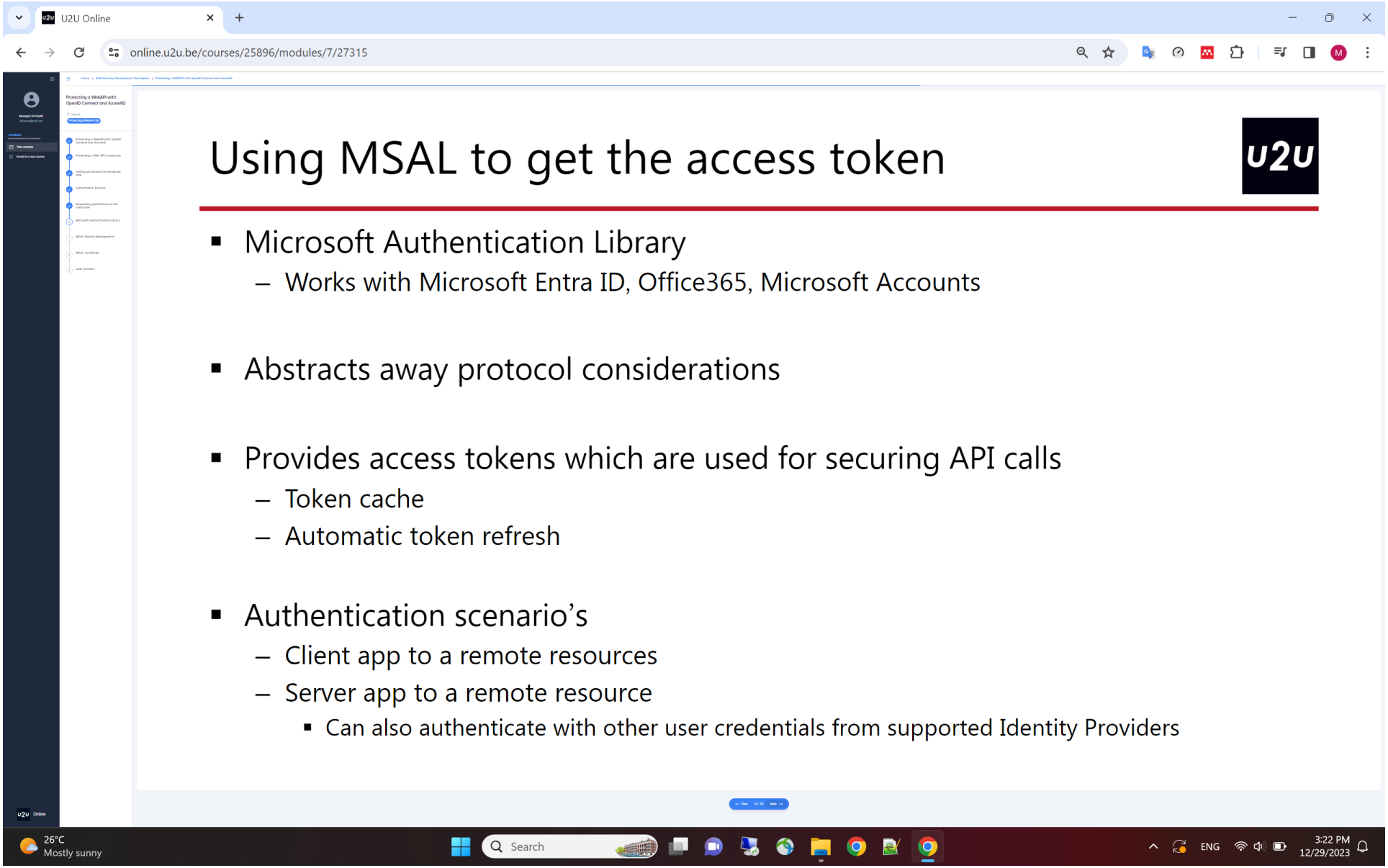

U2U Online
online.u2u.be/courses/25896/modules/7/27315
Step 1: Authenticate the client application
U2U
The client application needs to authenticate with AzureAD
For this a client secret is used
To generate the client secret in AzureAD
Open the Certificates & Secrets for the client application
Create a new key by entering (any) name, expiration
Certificates & secrets
API permissions
Expose an API
Owners
Manifest
Troubleshooting
Troubleshooting
New support request
THUMBPRINT
START DATE
EXPIRES
Client secrets
A secret string that the application uses to prove its identity when requesting a token. Also can be referred to as application password.
New client secret
DESCRIPTION
EXPIRES
VALUE
No description
7/18/2020
Hidden
Whatever I really Want
12/31/2299
3t3**********
26°C
Mostly sunny
Search
ENG
3:21 PM
12/29/2023

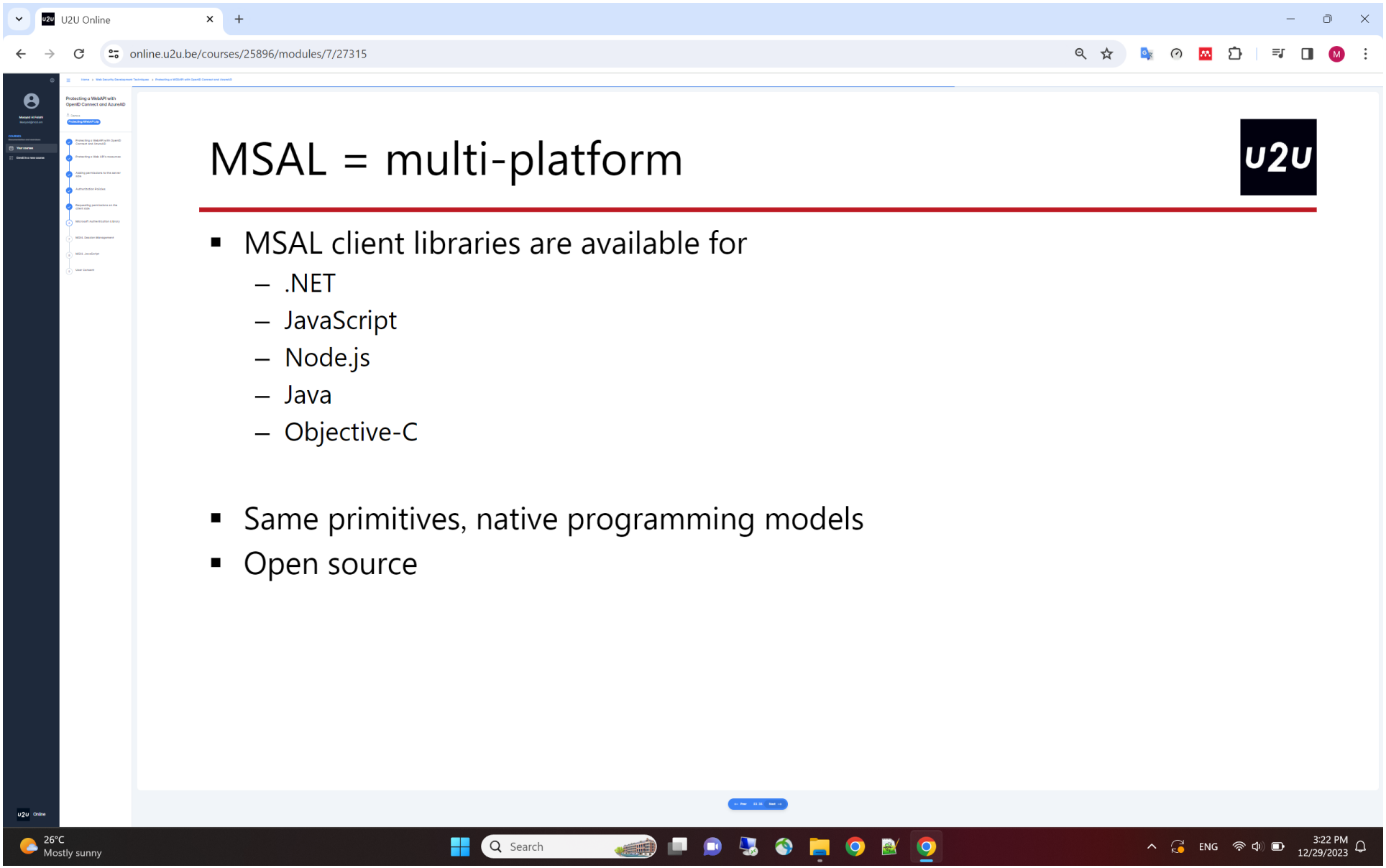

U2U Online
online.u2u.be/courses/25896/modules/7/27315
Step 2: Request code and access token
U2U
This step becomes very easy using Microsoft.Identity.Web
builder.Services.AddMicrosoftIdentityWebAppAuthentication(Configuration)
.EnableTokenAcquisitionToCallDownstreamApi(new string[] {})
.AddInMemoryTokenCaches();
26°C
Mostly sunny
Search
ENG
3:21 PM
12/29/2023

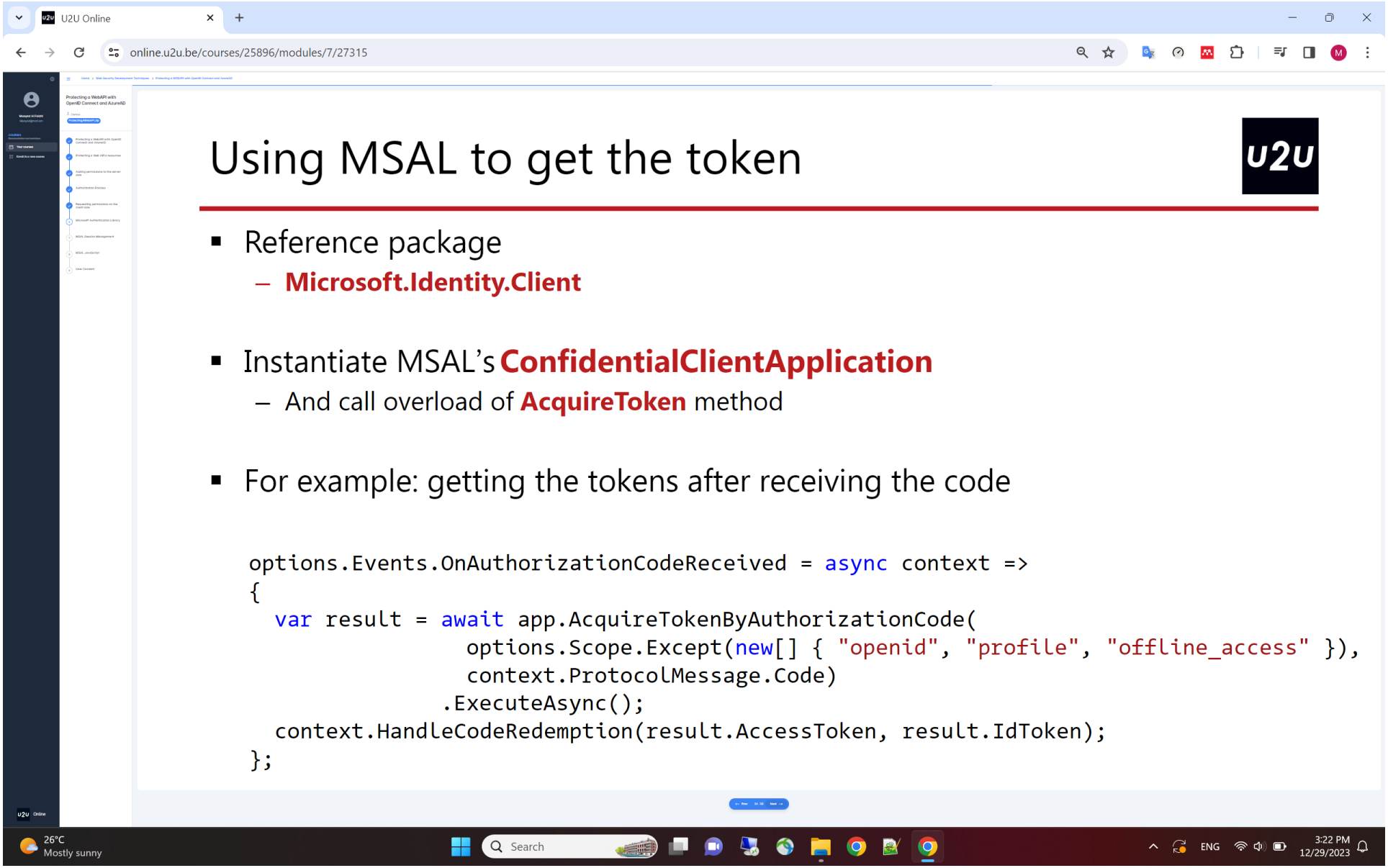

U2U Online
online.u2u.be/courses/25896/modules/7/27315
Step 3: Pass access token in Bearer token
u2u
Again, use MSAL to get access token (from cache)
Ensure you get the right user's cache!
Use the ITokenAcquisition service
var accessToken = await tokenAcquisition.GetAccessTokenForUserAsync()
26°C
Mostly sunny
Search
ENG
3:21 PM
12/29/2023

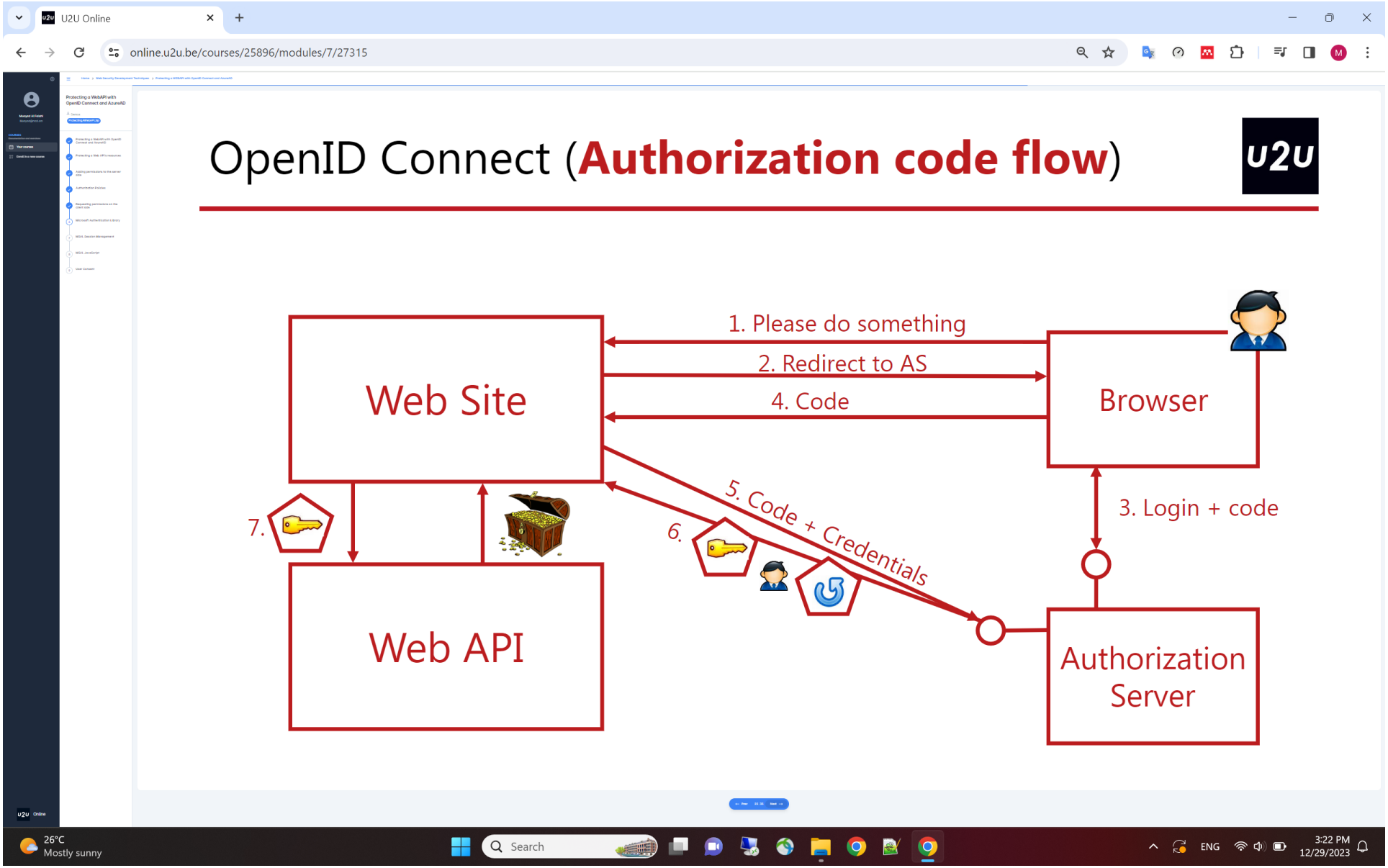

U2U Online
online.u2u.be/courses/25896/modules/7/27315
Step 3: Pass access token in Bearer token
U2U
Now pass access token in Bearer header
var client = new HttpClient();
client.DefaultRequestHeaders.Authorization =
new AuthenticationHeaderValue("Bearer", accessToken);
client.DefaultRequestHeaders.Accept.Add(
new MediaTypeWithQualityHeaderValue("application/json"));
var responseMessage = await client.GetAsync("https://localhost:44386/api/products");
26°C
Mostly sunny
Search
ENG
3:22 PM
12/29/2023

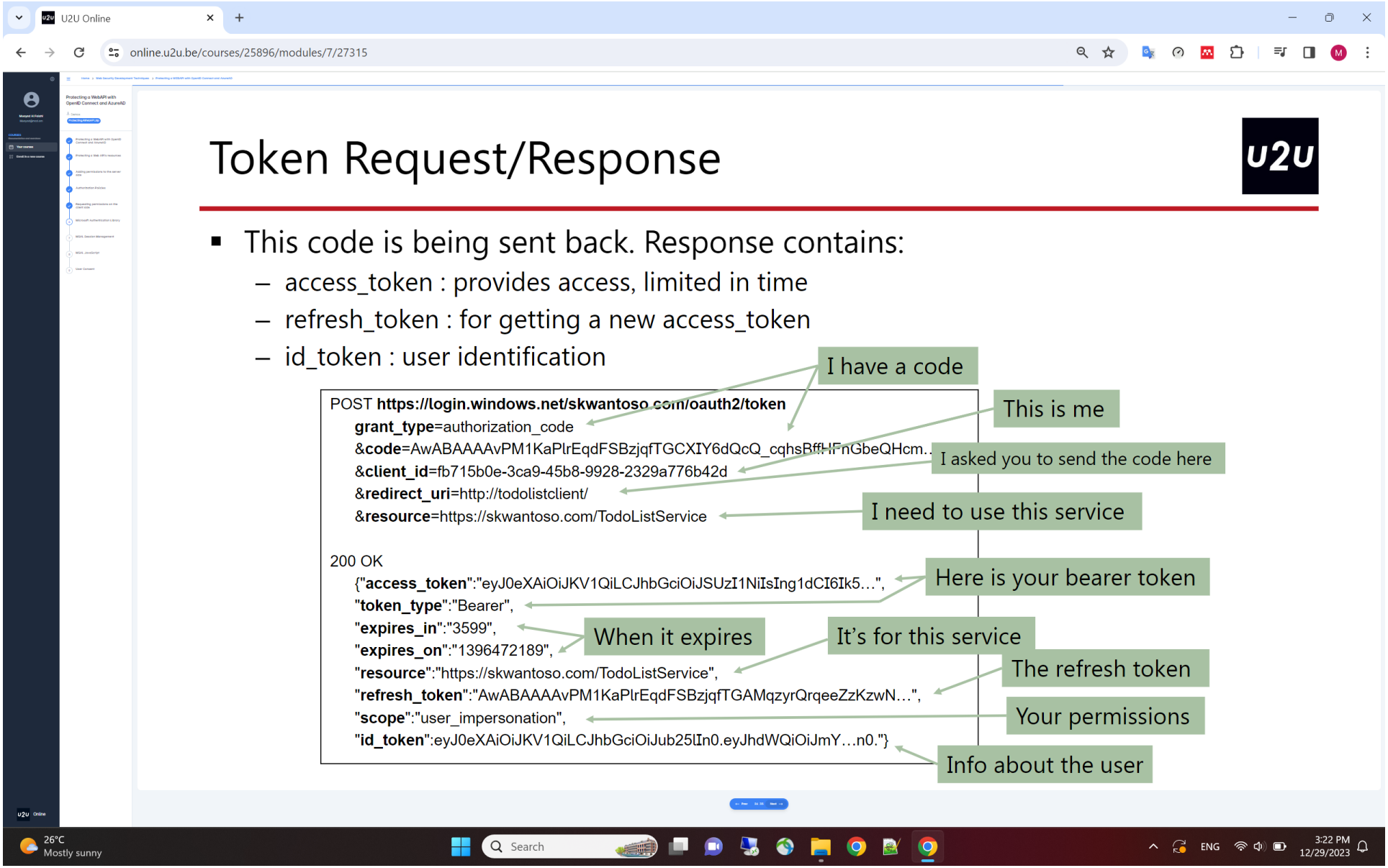

U2U Online
online.u2u.be/courses/25896/modules/7/27315
AuthorizeForScopes Attribute
U2U
The [AuthorizeForScopes] ensures that the user is asked for consent if needed, and incrementally
[AuthorizeForScopes(Scopes = new[] {
"api://dc68a11f-d265-4e9c-8a24-abbbd3520f8a/Mail.Send" })]
public async Task<IActionResult> SendEmail()
{
var accessToken = await tokenAcquisition.GetAccessTokenForUserAsync(
new[] { "api:// dc68a11f-d265-4e9c-8a24-abbbd3520f8a/Mail.Send" });
}
You can specify your scopes in configuration
[AuthorizeForScopes(ScopeKeySection = "Mails:MailsScope")]
26°C
Mostly sunny
Search
ENG
3:22 PM
12/29/2023

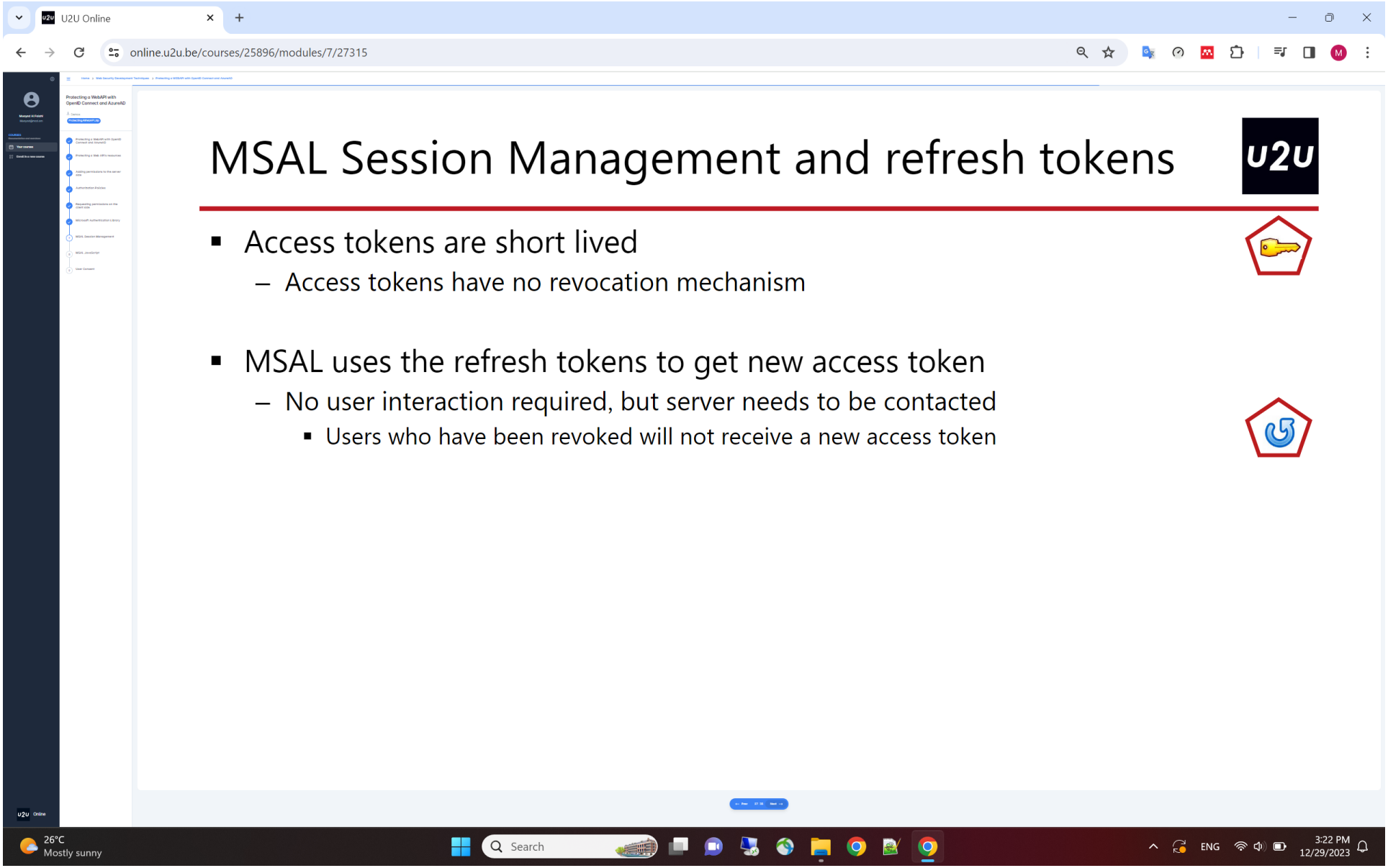

U2U Online
online.u2u.be/courses/25896/modules/7/27315
Using MSAL to get the access token
U2U
Microsoft Authentication Library
Works with Microsoft Entra ID, Office365, Microsoft Accounts
Abstracts away protocol considerations
Provides access tokens which are used for securing API calls
Token cache
Automatic token refresh
Authentication scenario's
Client app to a remote resources
Server app to a remote resource
Can also authenticate with other user credentials from supported Identity Providers
26°C
Mostly sunny
Search
ENG
3:22 PM
12/29/2023

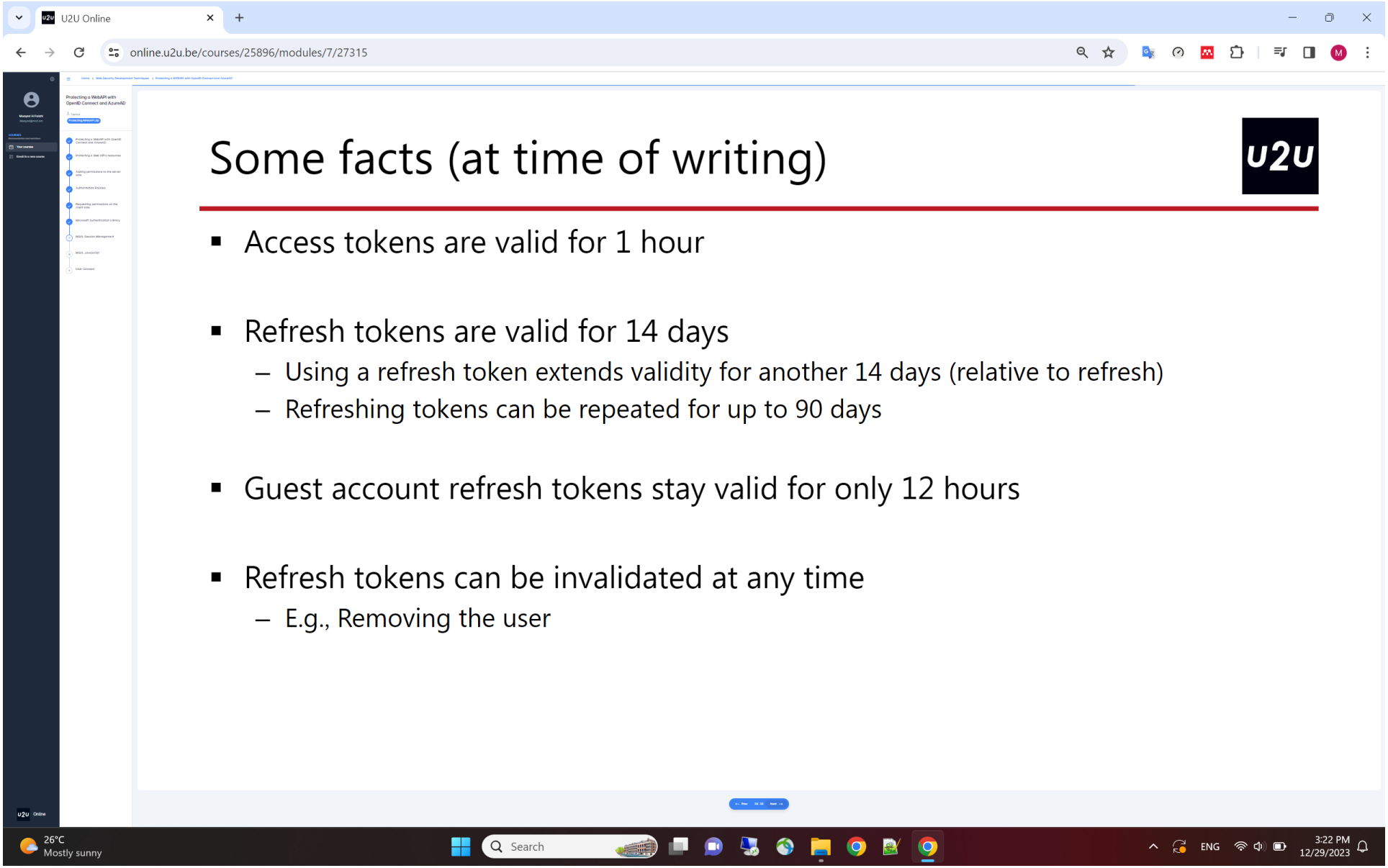

U2U Online
online.u2u.be/courses/25896/modules/7/27315
MSAL = multi-platform
u2u
MSAL client libraries are available for
.NET
JavaScript
Node.js
Java
Objective-C
Same primitives, native programming models
Open source
26°C
Mostly sunny
Search
ENG
3:22 PM
12/29/2023

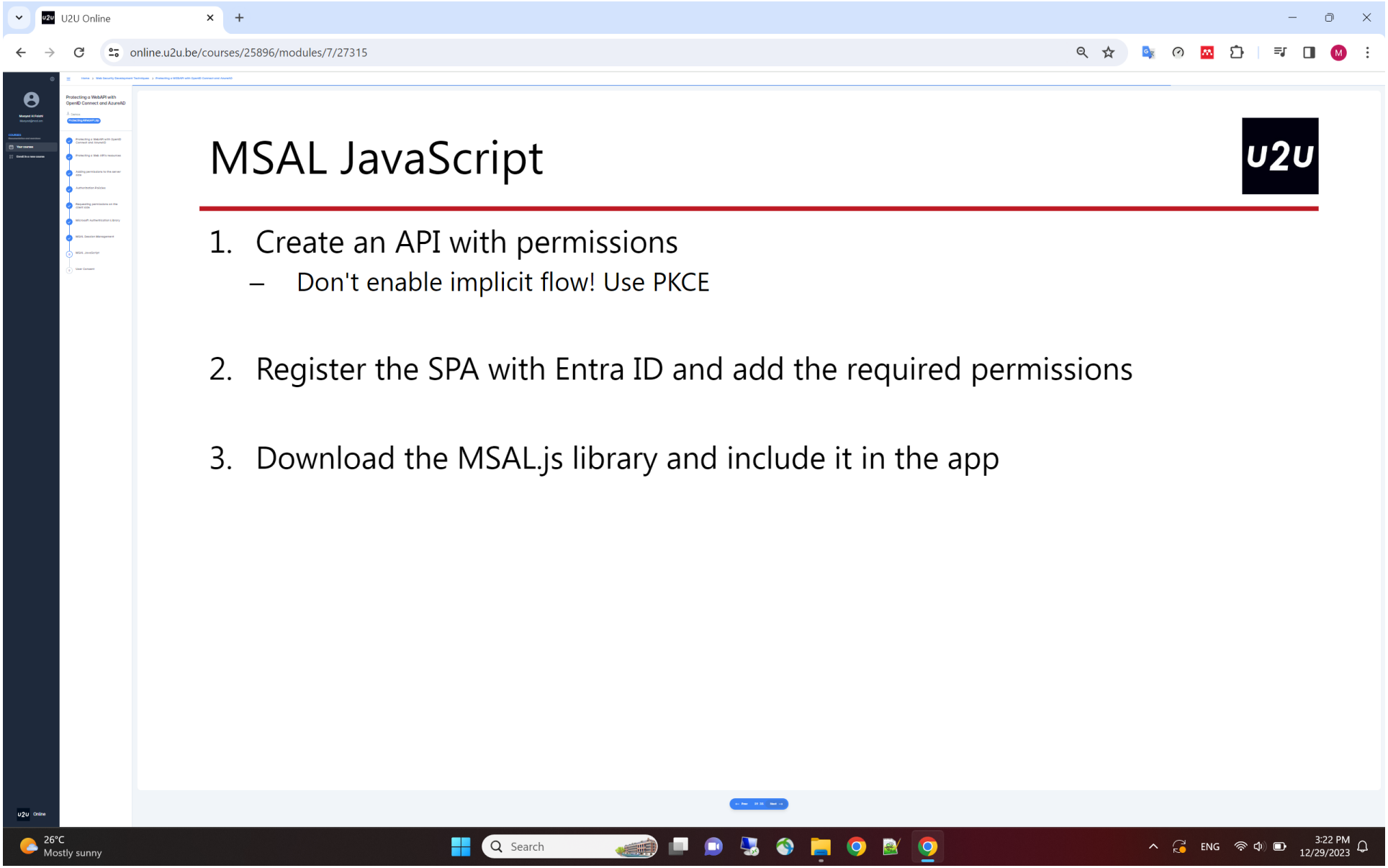

U2U Online
online.u2u.be/courses/25896/modules/7/27315
Using MSAL to get the token
U2U
Reference package
Microsoft.Identity.Client
Instantiate MSAL's ConfidentialClientApplication
And call overload of AcquireToken method
For example: getting the tokens after receiving the code
options.Events.OnAuthorizationCodeReceived = async context =>
{
var result = await app.AcquireTokenByAuthorizationCode(
options.Scope.Except(new[] { "openid", "profile", "offline_access" }),
context.ProtocolMessage.Code)
.ExecuteAsync();
context.HandleCodeRedemption(result.AccessToken, result.IdToken);
};
26°C
Mostly sunny
Search
ENG
3:22 PM
12/29/2023

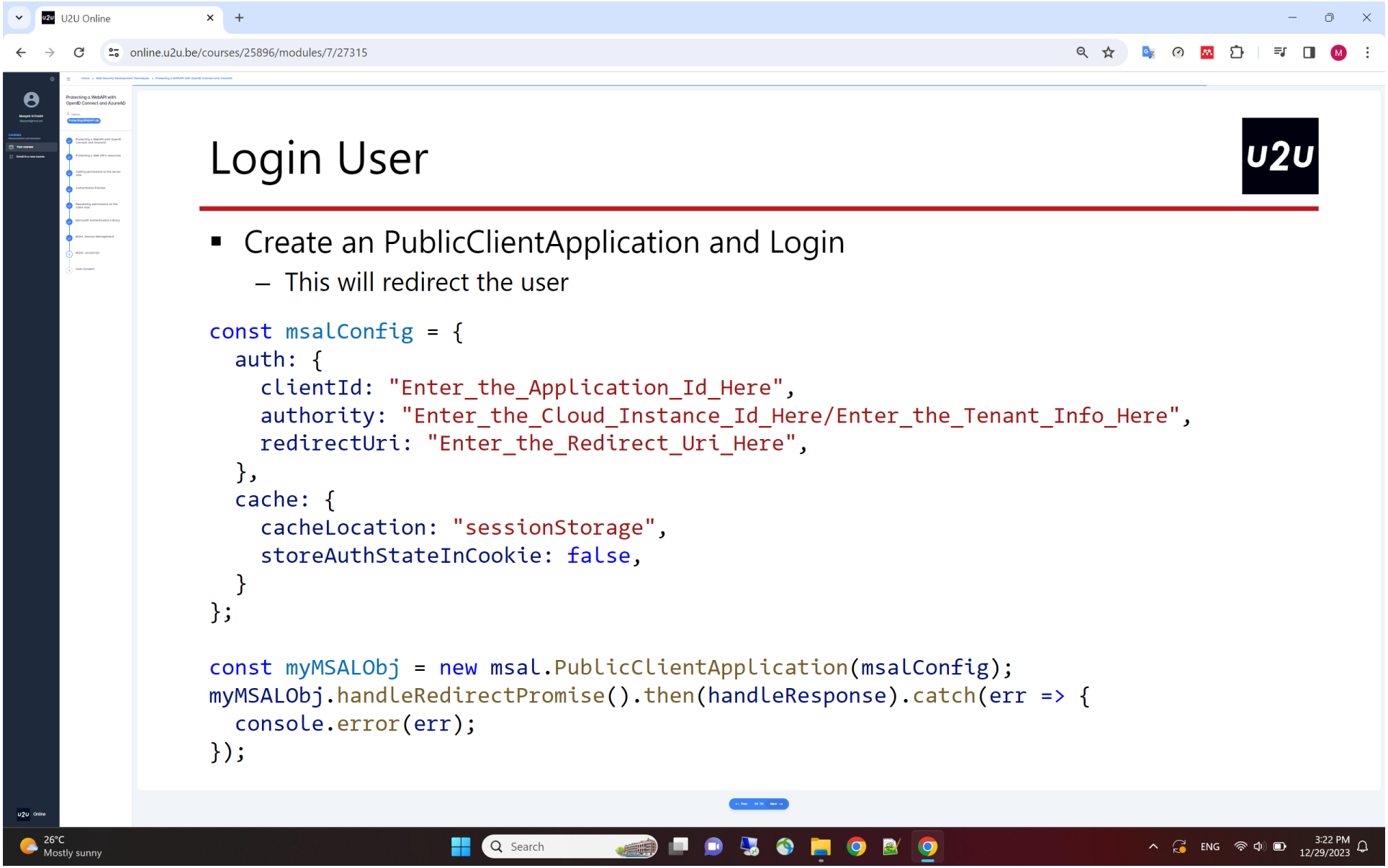

U2U Online
online.u2u.be/courses/25896/modules/7/27315
OpenID Connect (Authorization code flow)
U2U
Web Site
Web API
Browser
Authorization Server
1. Please do something
2. Redirect to AS
4. Code
5. Code + Credentials
6.
7.
3. Login + code
26°C
Mostly sunny
Search
ENG
3:22 PM
12/29/2023

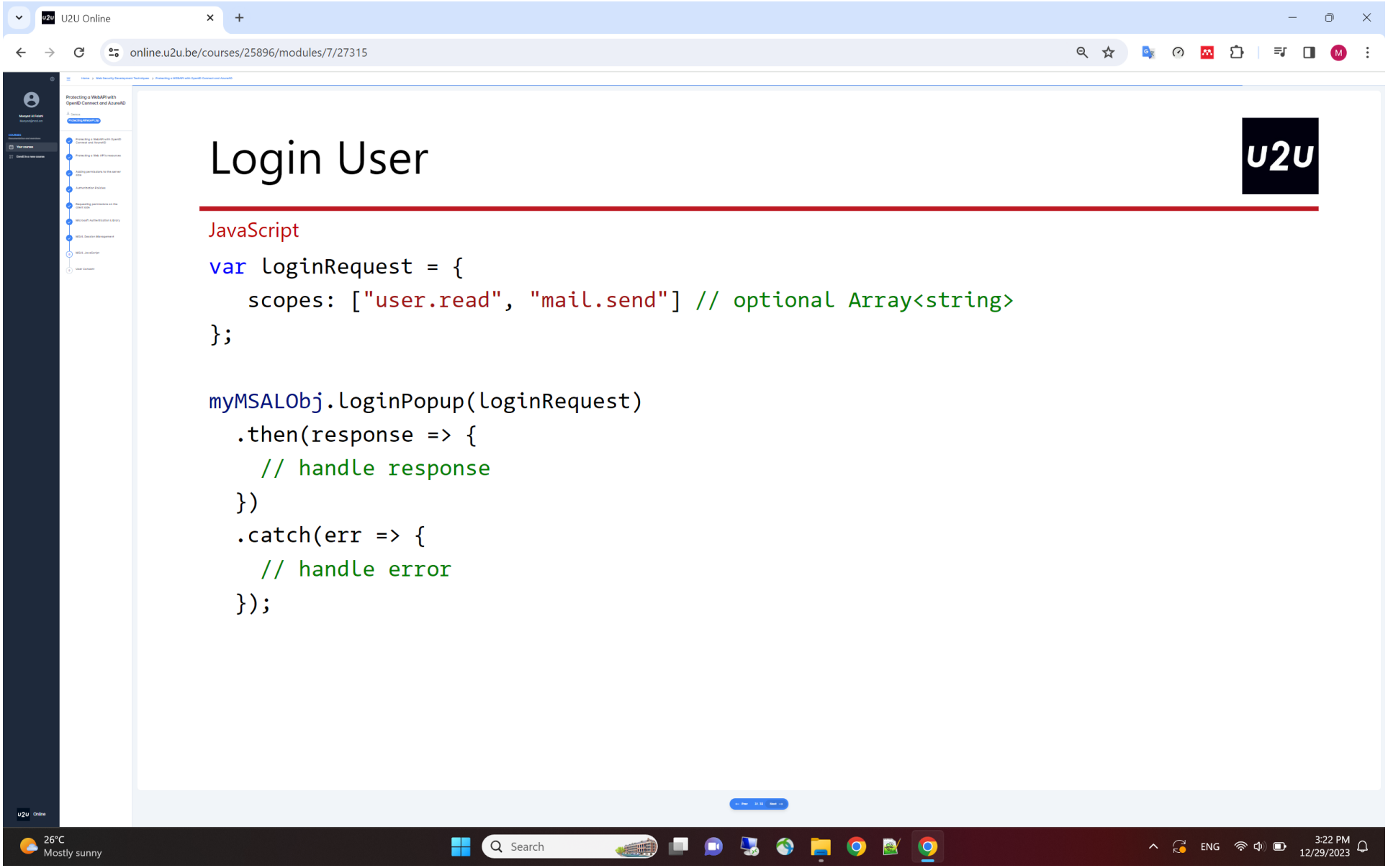

U2U Online
online.u2u.be/courses/25896/modules/7/27315
Token Request/Response
u2u
This code is being sent back. Response contains:
access_token : provides access, limited in time
refresh_token : for getting a new access_token
id_token : user identification
I have a code
This is me
I asked you to send the code here
I need to use this service
Here is your bearer token
When it expires
It's for this service
The refresh token
Your permissions
Info about the user
POST https://login.windows.net/skwantoso.com/oauth2/token
grant_type=authorization_code
&code=AwABAAAAvPM1KaPlrEqdFSBzjqfTGCXIY6dQcQ_cqhsBffHFnGbeQHcm..
&client_id=fb715b0e-3ca9-45b8-9928-2329a776b42d
&redirect_uri=http://todolistclient/
&resource=https://skwantoso.com/TodoListService
200 OK
{"access_token":"eyJ0eXAiOiJKV1QiLCJhbGciOiJSUzI1NiIsIng1dCI6Ik5…",
"token_type":"Bearer",
"expires_in":"3599",
"expires_on":"1396472189",
"resource":"https://skwantoso.com/TodoListService",
"refresh_token":"AwABAAAAvPM1KaPlrEqdFSBzjqfTGAMqzyrQrqeeZzKzwN…",
"scope":"user_impersonation",
"id_token":eyJ0eXAiOiJKV1QiLCJhbGciOiJub25lIn0.eyJhdWQiOiJmY…n0."}
26°C
Mostly sunny
Search
ENG
3:22 PM
12/29/2023

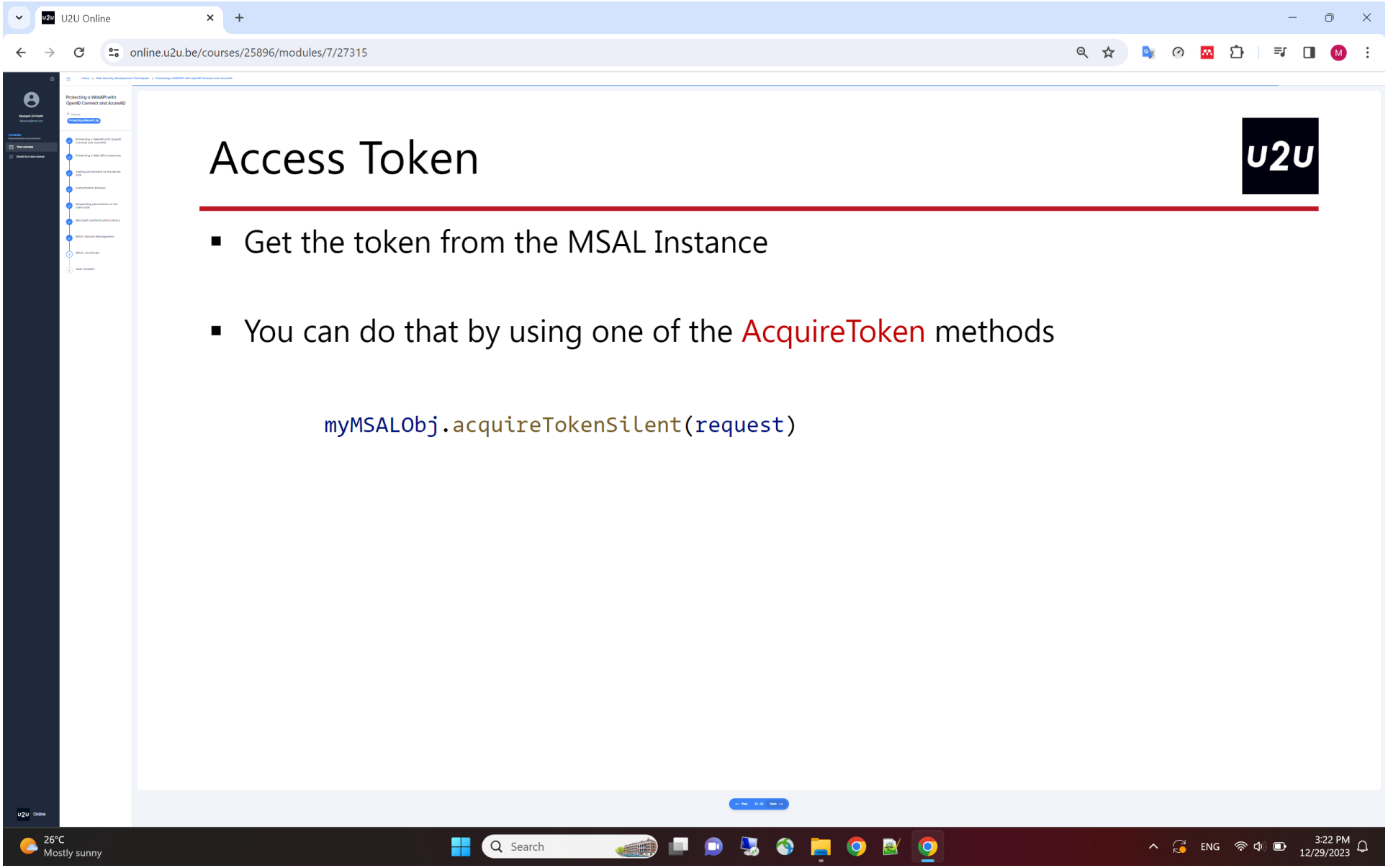

U2U Online
online.u2u.be/courses/25896/modules/7/27315
MSAL Session Management and refresh tokens
u2u
Access tokens are short lived
Access tokens have no revocation mechanism
MSAL uses the refresh tokens to get new access token
No user interaction required, but server needs to be contacted
Users who have been revoked will not receive a new access token
26°C
Mostly sunny
Search
ENG
3:22 PM
12/29/2023

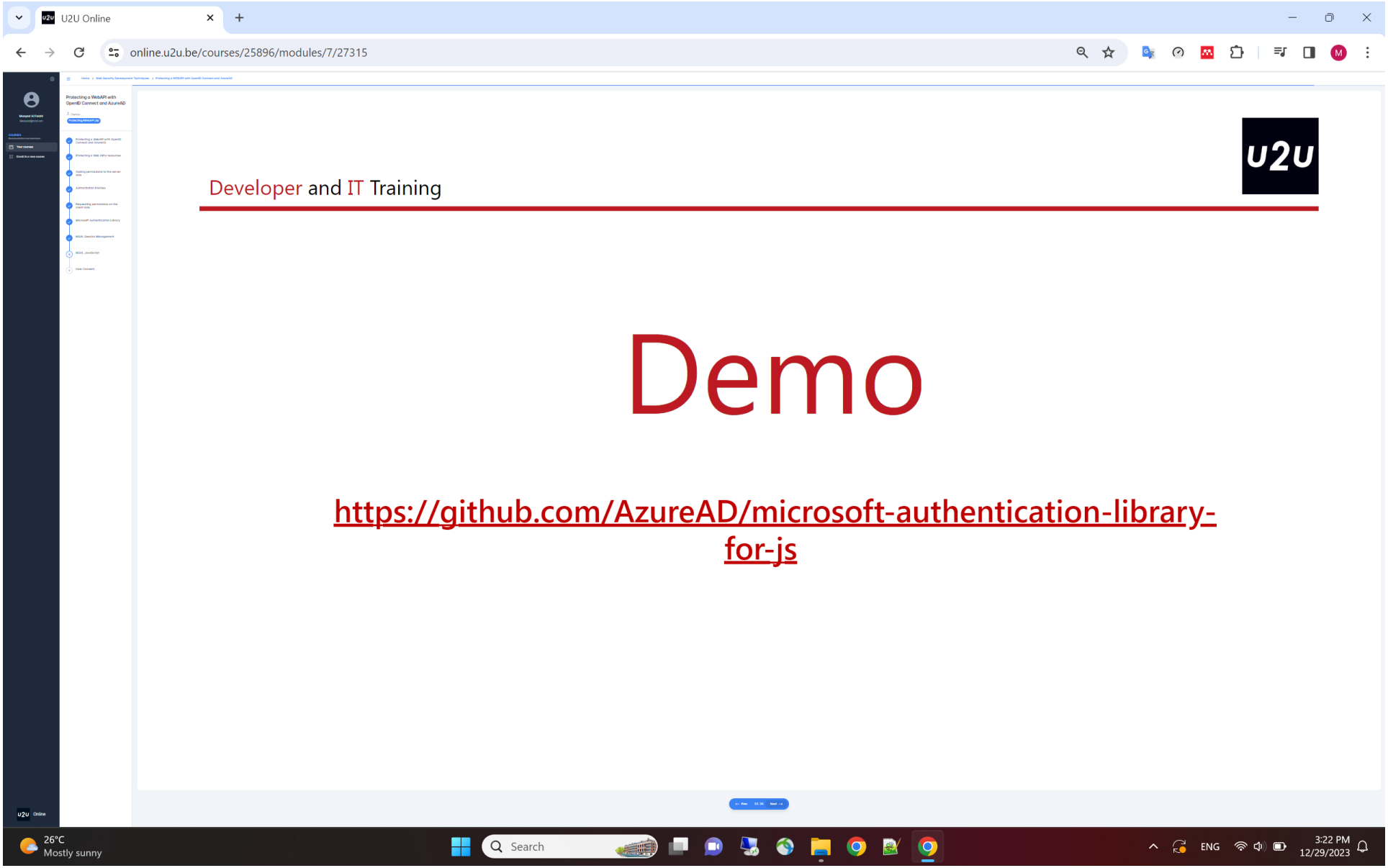

U2U Online
online.u2u.be/courses/25896/modules/7/27315
Some facts (at time of writing)
U2U
Access tokens are valid for 1 hour
Refresh tokens are valid for 14 days
Using a refresh token extends validity for another 14 days (relative to refresh)
Refreshing tokens can be repeated for up to 90 days
Guest account refresh tokens stay valid for only 12 hours
Refresh tokens can be invalidated at any time
E.g., Removing the user
26°C
Mostly sunny
Search
ENG
3:22 PM
12/29/2023

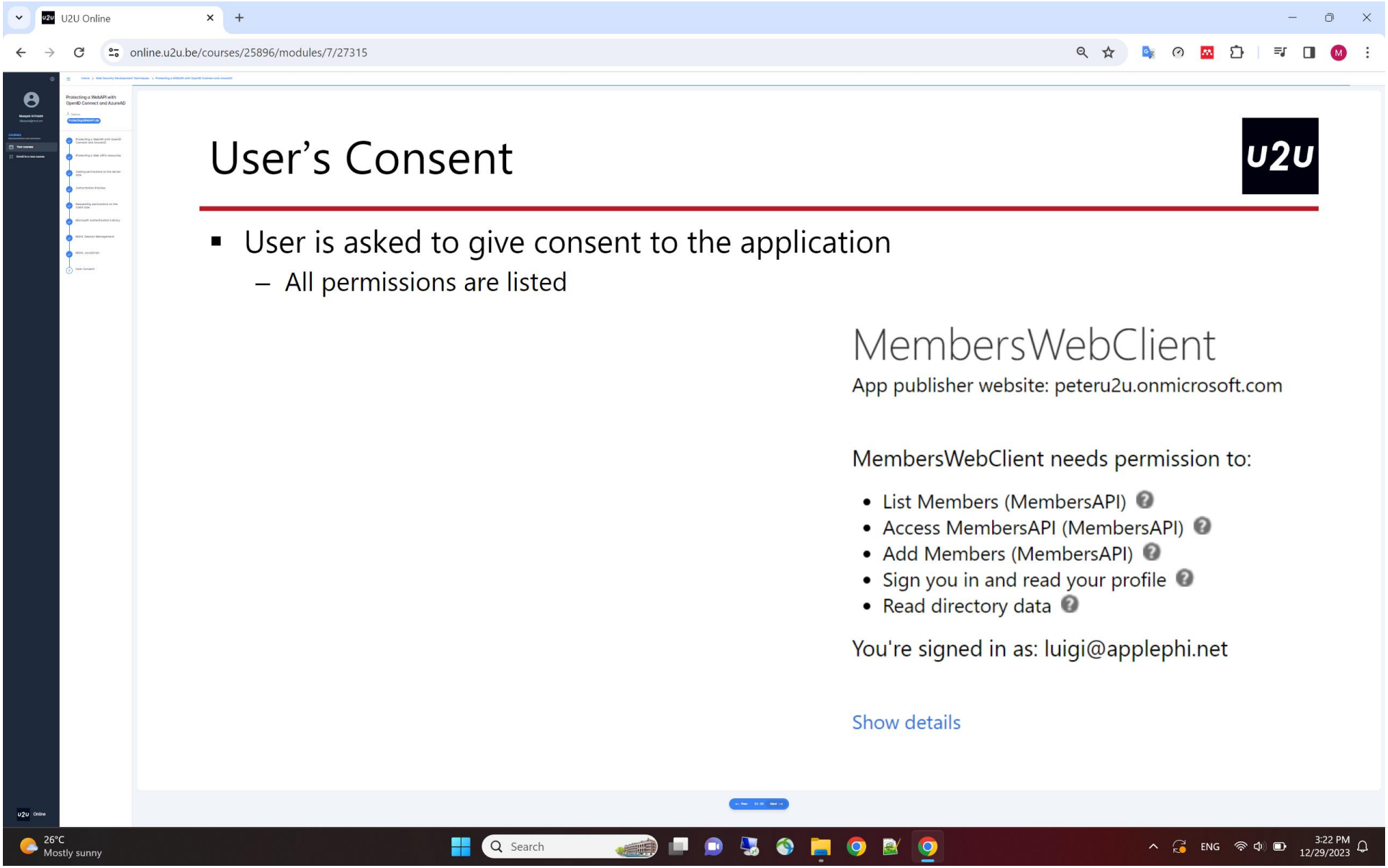

U2U Online
online.u2u.be/courses/25896/modules/7/27315
MSAL JavaScript
u2u
1. Create an API with permissions
– Don't enable implicit flow! Use PKCE
2. Register the SPA with Entra ID and add the required permissions
3. Download the MSAL.js library and include it in the app
26°C
Mostly sunny
Search
ENG
3:22 PM
12/29/2023

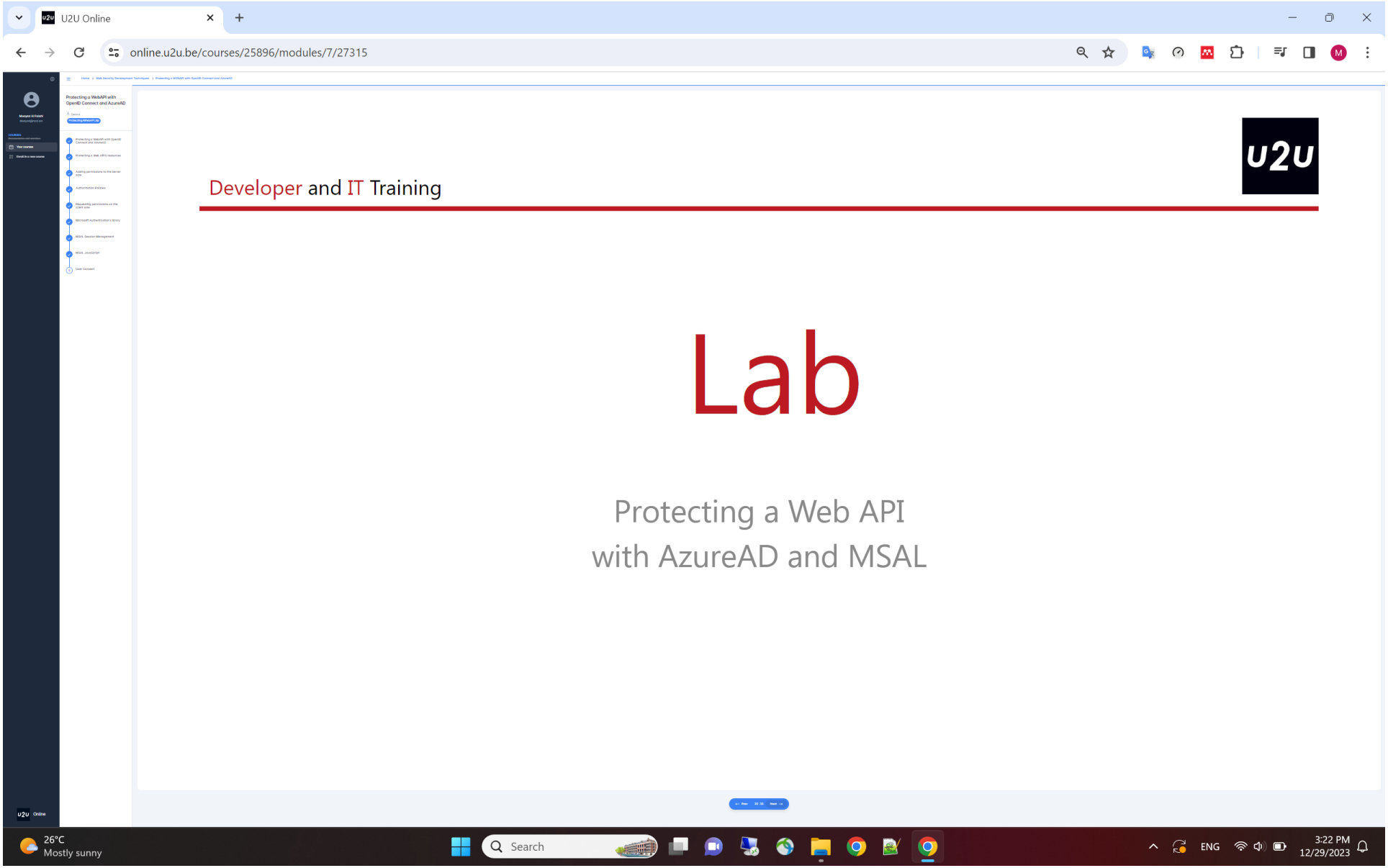

U2U Online
online.u2u.be/courses/25896/modules/7/27315
Login User
U2U
Create an PublicClientApplication and Login
This will redirect the user
const msalConfig = {
auth: {
clientId: "Enter_the_Application_Id_Here",
authority: "Enter_the_Cloud_Instance_Id_Here/Enter_the_Tenant_Info_Here",
redirectUri: "Enter_the_Redirect_Uri_Here",
},
cache: {
cacheLocation: "sessionStorage",
storeAuthStateInCookie: false,
}
};
const myMSALObj = new msal.PublicClientApplication(msalConfig);
myMSALObj.handleRedirectPromise().then(handleResponse).catch(err => {
console.error(err);
});
26°C
Mostly sunny
Search
ENG
3:22 PM
12/29/2023


U2U Online
online.u2u.be/courses/25896/modules/7/27315
Login User
u2u
JavaScript
var loginRequest = {
scopes: ["user.read", "mail.send"] // optional Array<string>
};
myMSALObj.loginPopup(loginRequest)
.then(response => {
// handle response
})
.catch(err => {
// handle error
});
26°C
Mostly sunny
Search
ENG
3:22 PM
12/29/2023


U2U Online
online.u2u.be/courses/25896/modules/7/27315
Access Token
u2u
Get the token from the MSAL Instance
You can do that by using one of the AcquireToken methods
myMSALObj.acquireTokenSilent(request)
26°C
Mostly sunny
Search
ENG
3:22 PM
12/29/2023


U2U Online
online.u2u.be/courses/25896/modules/7/27315
Developer and IT Training
u2u
Demo
https://github.com/AzureAD/microsoft-authentication-library-for-js
26°C
Mostly sunny
Search
ENG
3:22 PM
12/29/2023


U2U Online
online.u2u.be/courses/25896/modules/7/27315
User's Consent
U2U
User is asked to give consent to the application
All permissions are listed
MembersWebClient
App publisher website: peteru2u.onmicrosoft.com
MembersWebClient needs permission to:
List Members (MembersAPI)
Access MembersAPI (MembersAPI)
Add Members (MembersAPI)
Sign you in and read your profile
Read directory data
You're signed in as: luigi@applephi.net
Show details
26°C
Mostly sunny
Search
ENG
3:22 PM
12/29/2023


U2U Online
online.u2u.be/courses/25896/modules/7/27315
Developer and IT Training
u2u
Lab
Protecting a Web API
with AzureAD and MSAL
26°C
Mostly sunny
Search
ENG
3:22 PM
12/29/2023