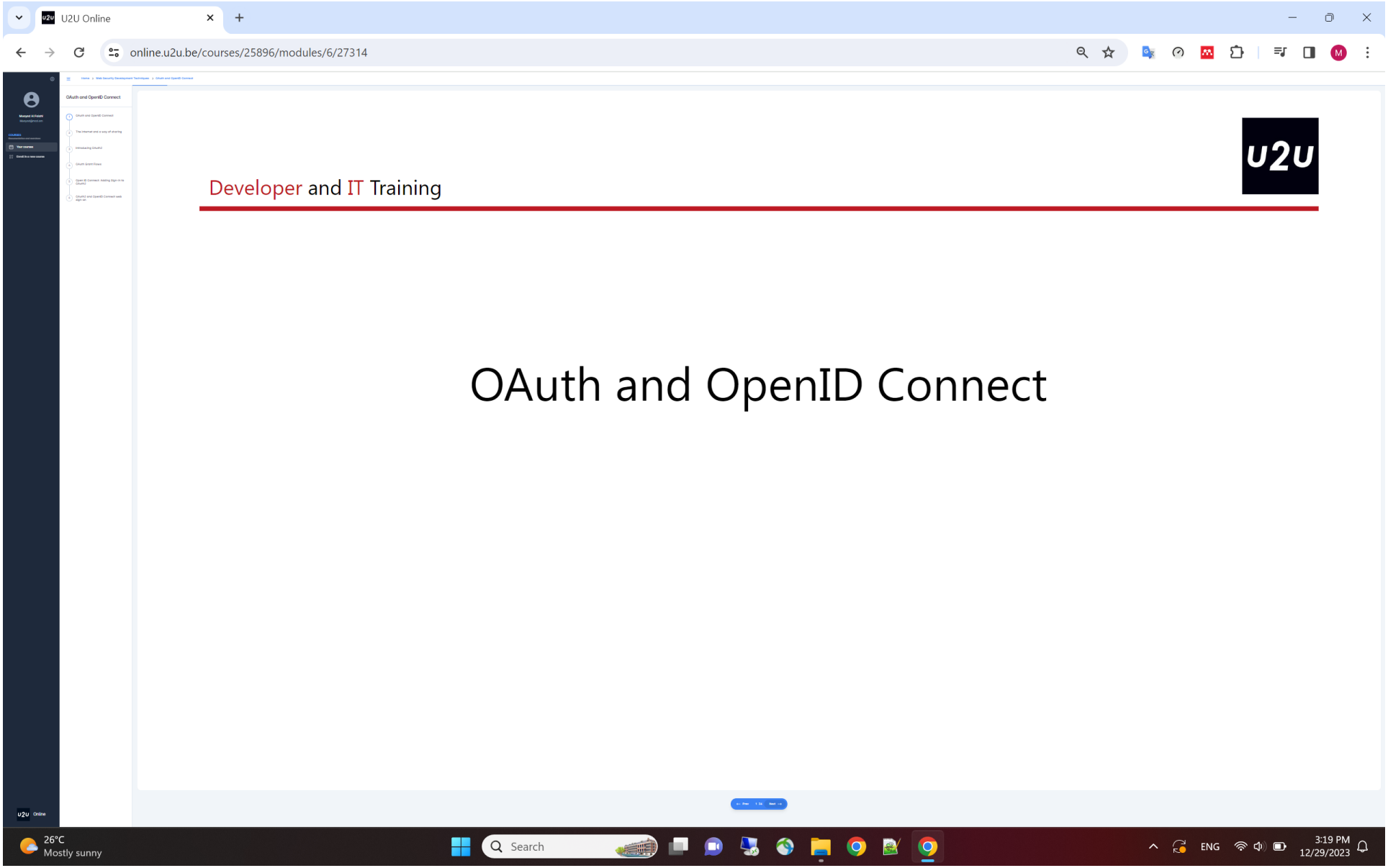
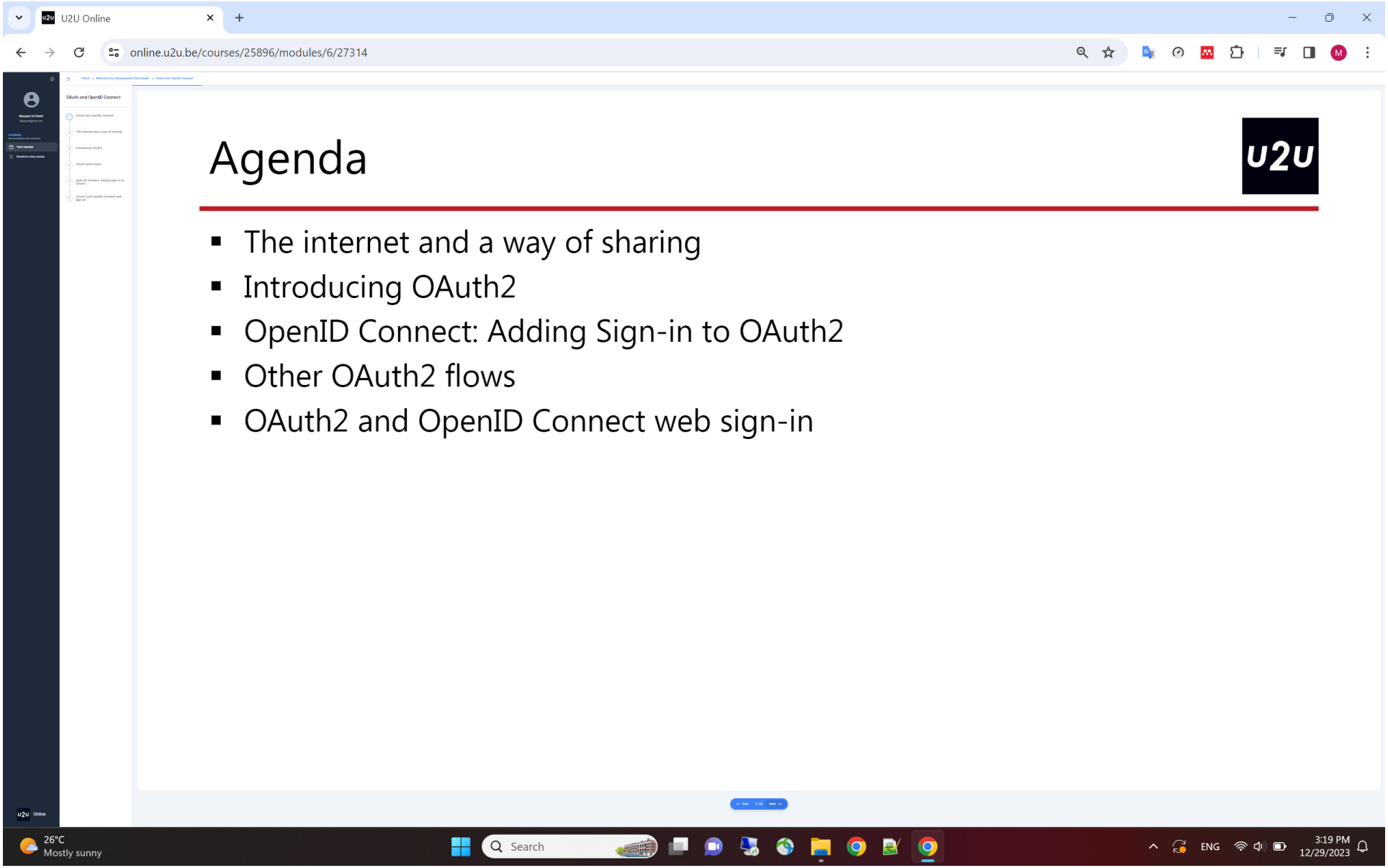
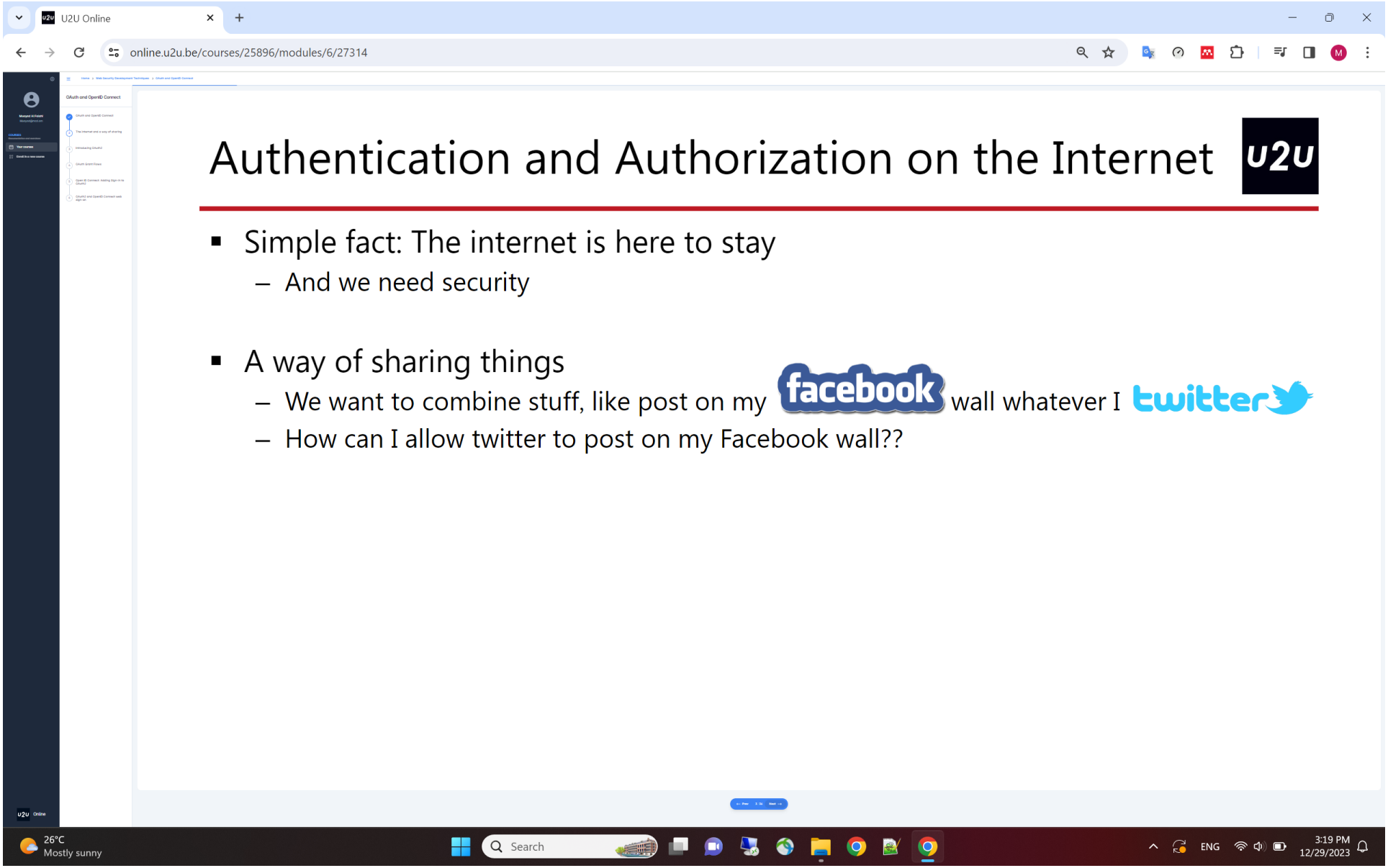

U2U Online
online.u2u.be/courses/25896/modules/6/27314
Developer and IT Training
OAuth and OpenID Connect
26°C
Mostly sunny
Search
ENG
3:19 PM
12/29/2023


U2U Online
online.u2u.be/courses/25896/modules/6/27314
Agenda
u2u
The internet and a way of sharing
Introducing OAuth2
OpenID Connect: Adding Sign-in to OAuth2
Other OAuth2 flows
OAuth2 and OpenID Connect web sign-in
26°C
Mostly sunny
Search
ENG
3:19 PM
12/29/2023


U2U Online
online.u2u.be/courses/25896/modules/6/27314
Authentication and Authorization on the Internet
U2U
Simple fact: The internet is here to stay
And we need security
A way of sharing things
We want to combine stuff, like post on my facebook wall whatever I twitter
How can I allow twitter to post on my Facebook wall??
26°C
Mostly sunny
Search
ENG
3:19 PM
12/29/2023

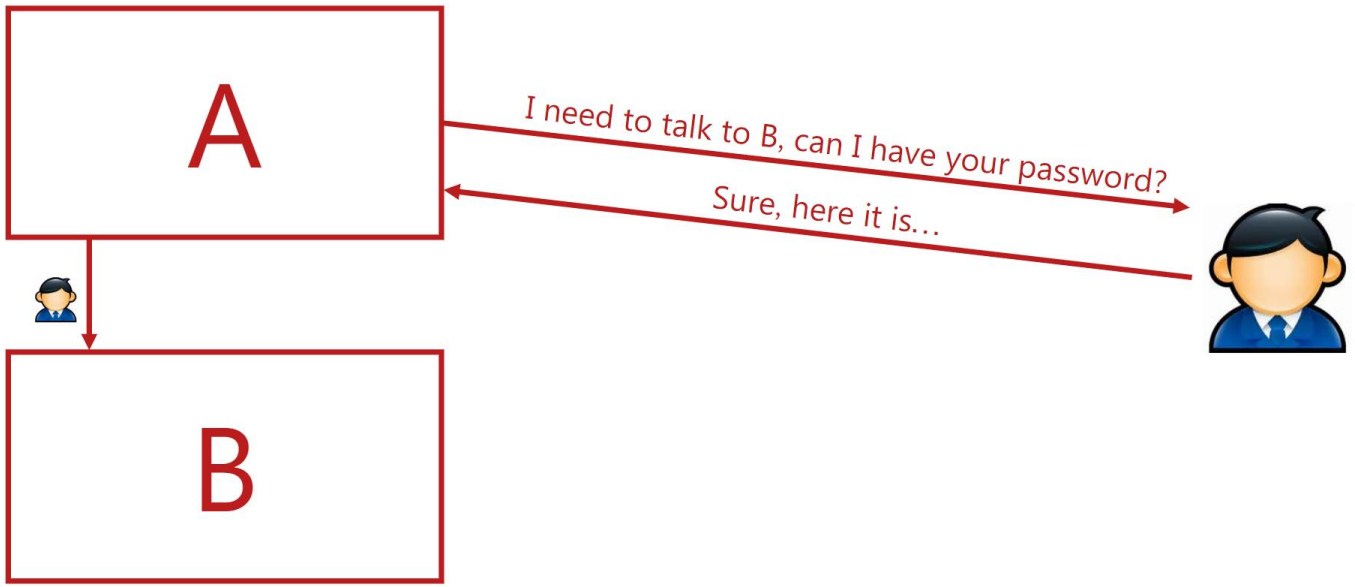
U2U Online

online.u2u.be/courses/25896/modules/6/27314

Password sharing?

U2U

- Simple idea – huge anti-pattern

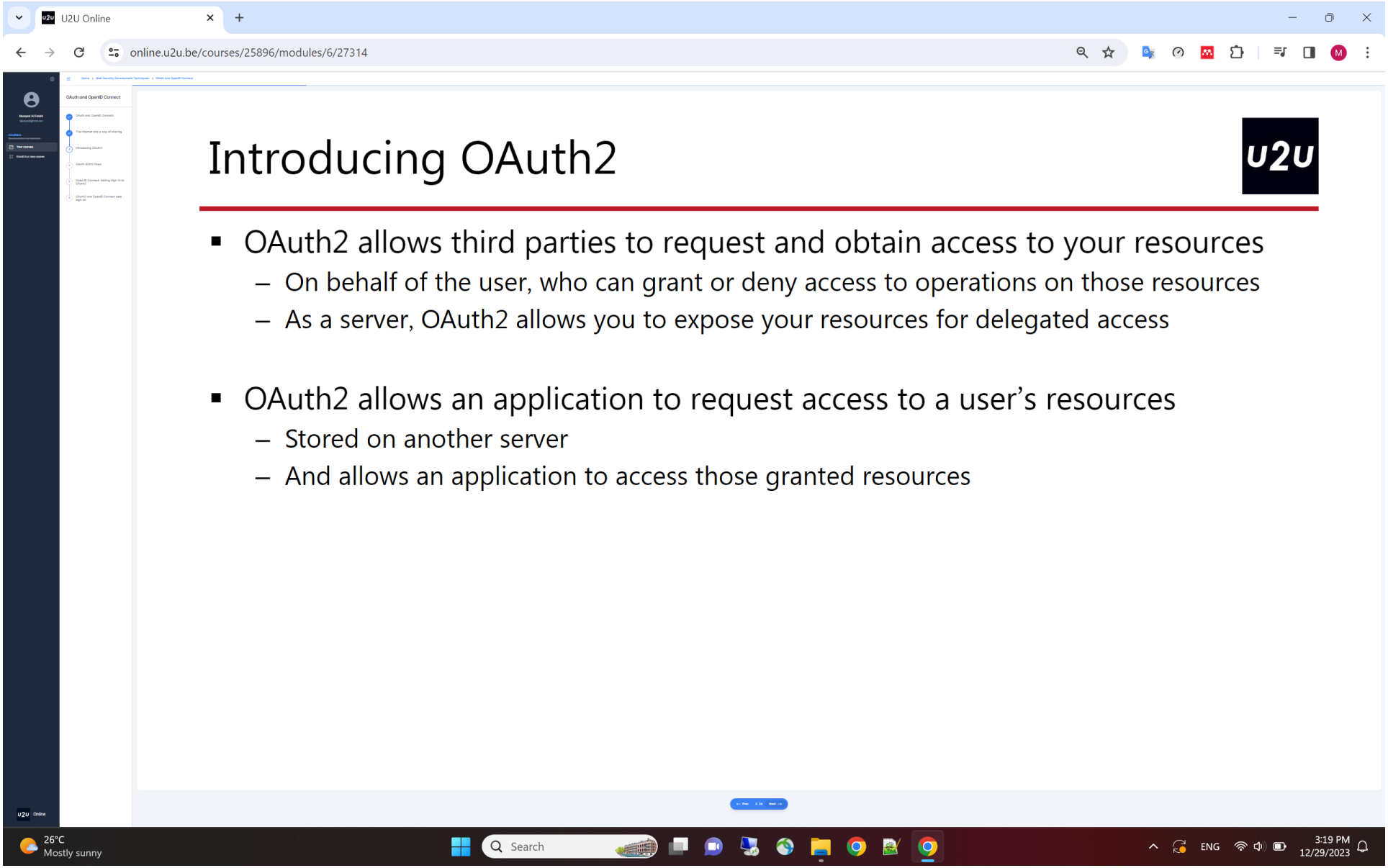


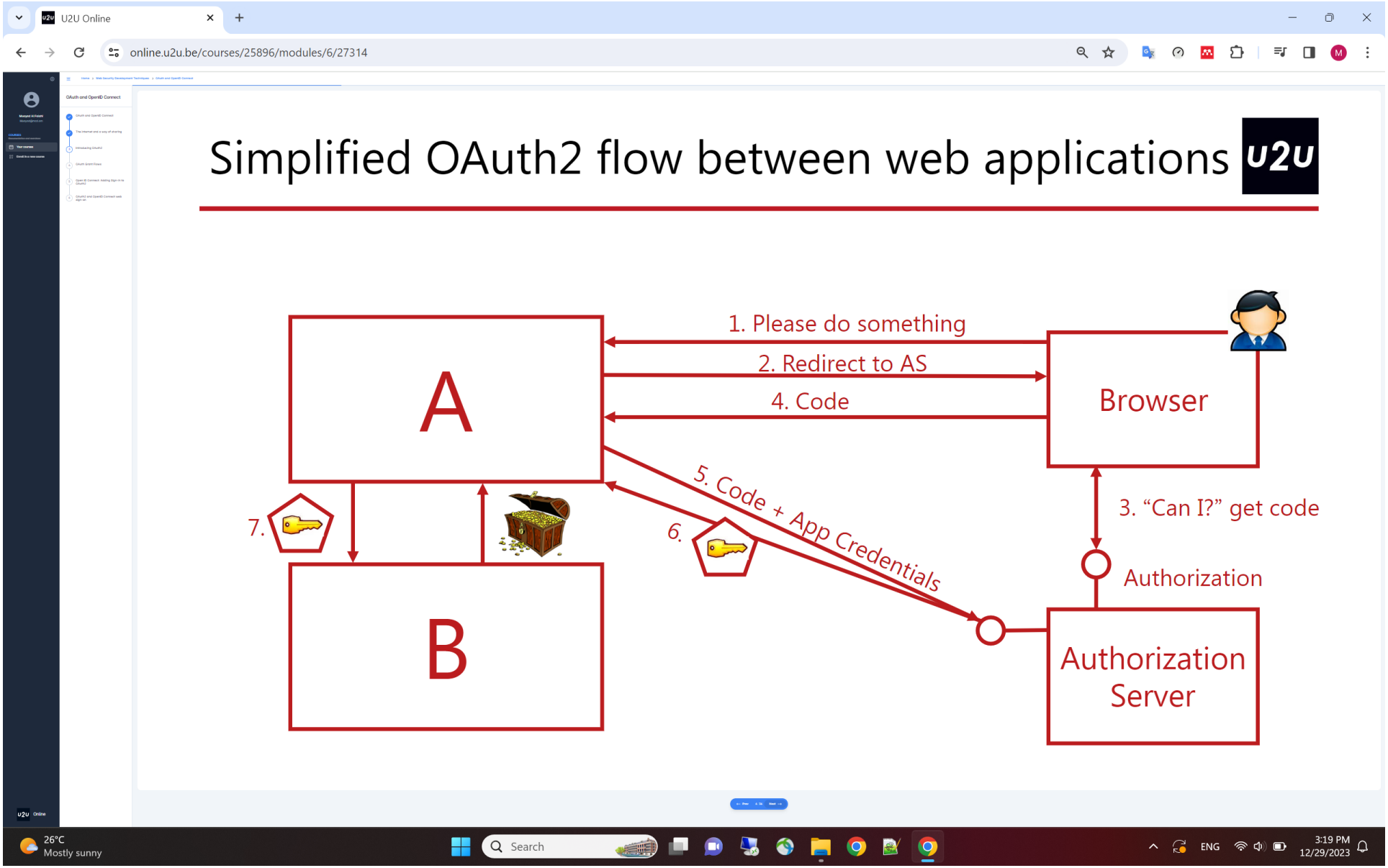
26°C
Mostly sunny

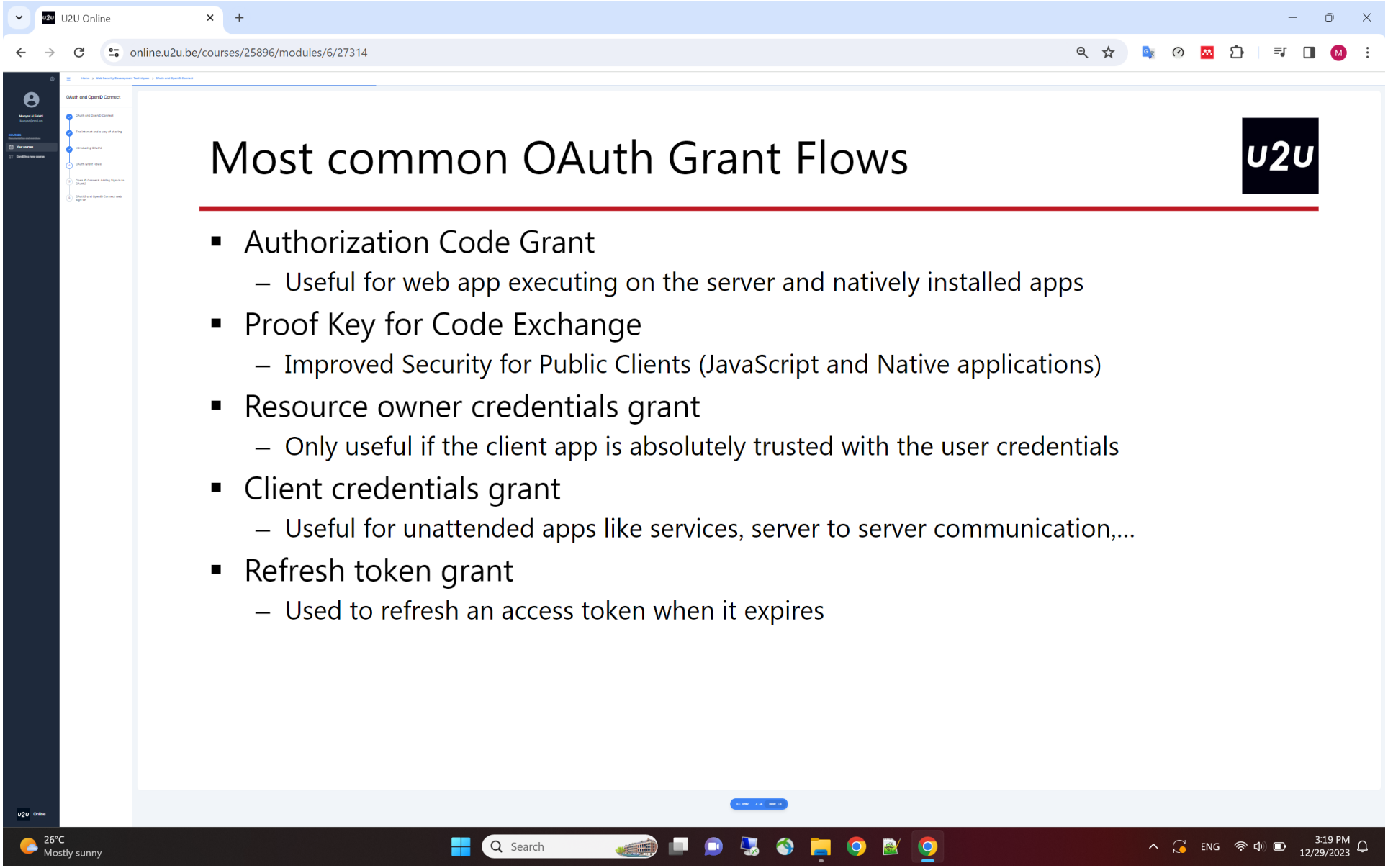
Search

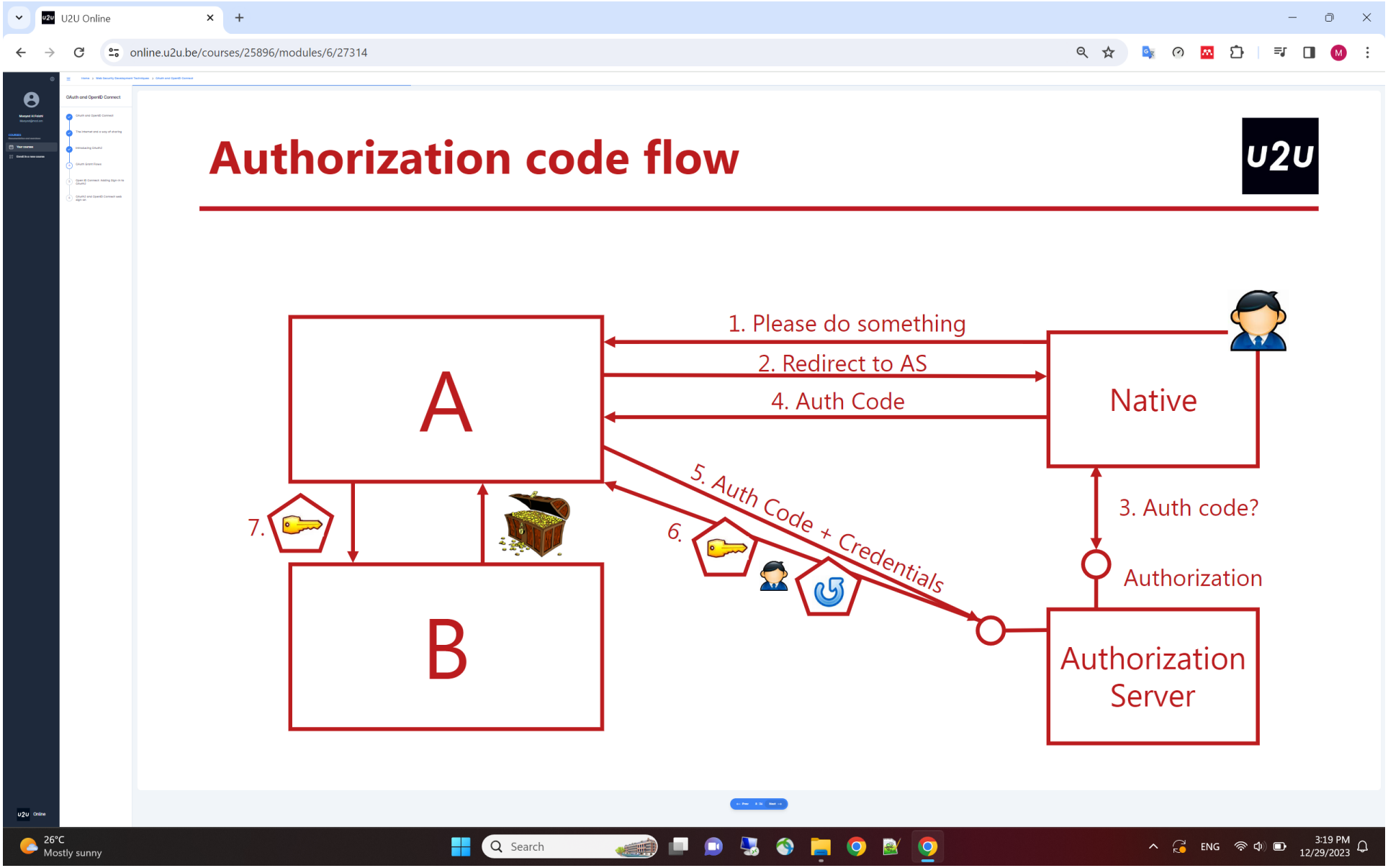
ENG

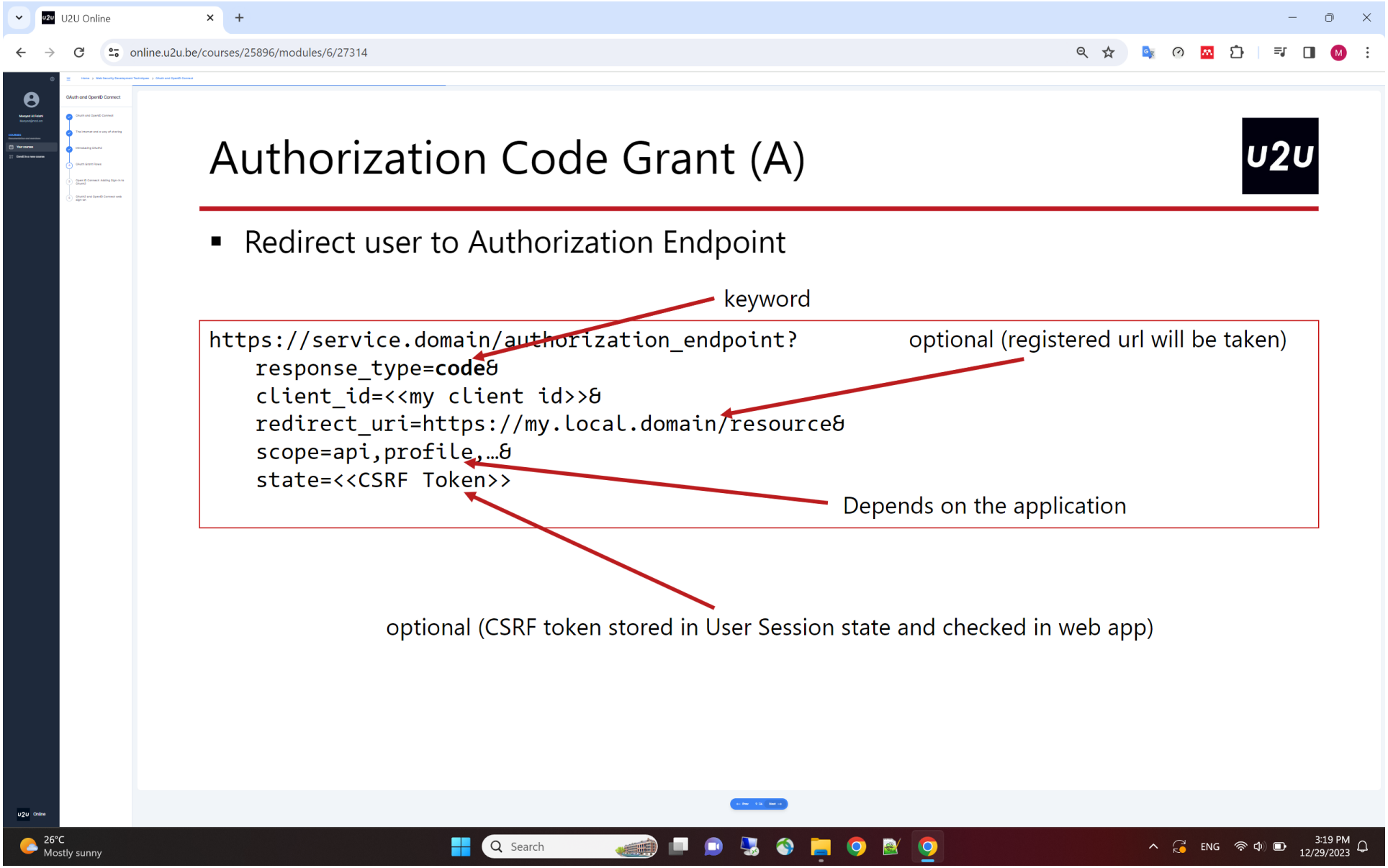
3:19 PM
12/29/2023

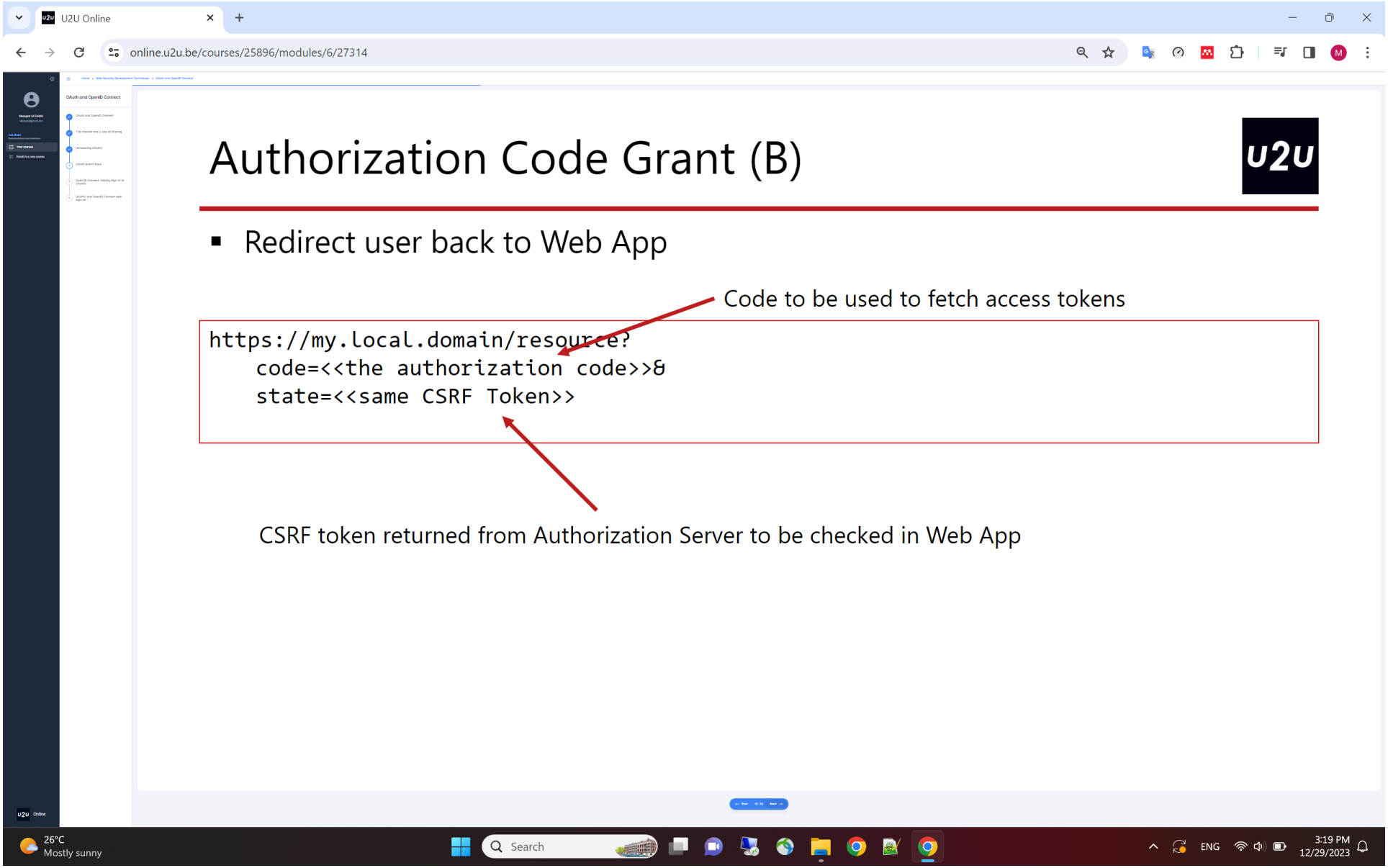

U2U Online
online.u2u.be/courses/25896/modules/6/27314
Introducing OAuth2
u2u
OAuth2 allows third parties to request and obtain access to your resources
On behalf of the user, who can grant or deny access to operations on those resources
As a server, OAuth2 allows you to expose your resources for delegated access
OAuth2 allows an application to request access to a user's resources
Stored on another server
And allows an application to access those granted resources
26°C
Mostly sunny
Search
ENG
3:19 PM
12/29/2023

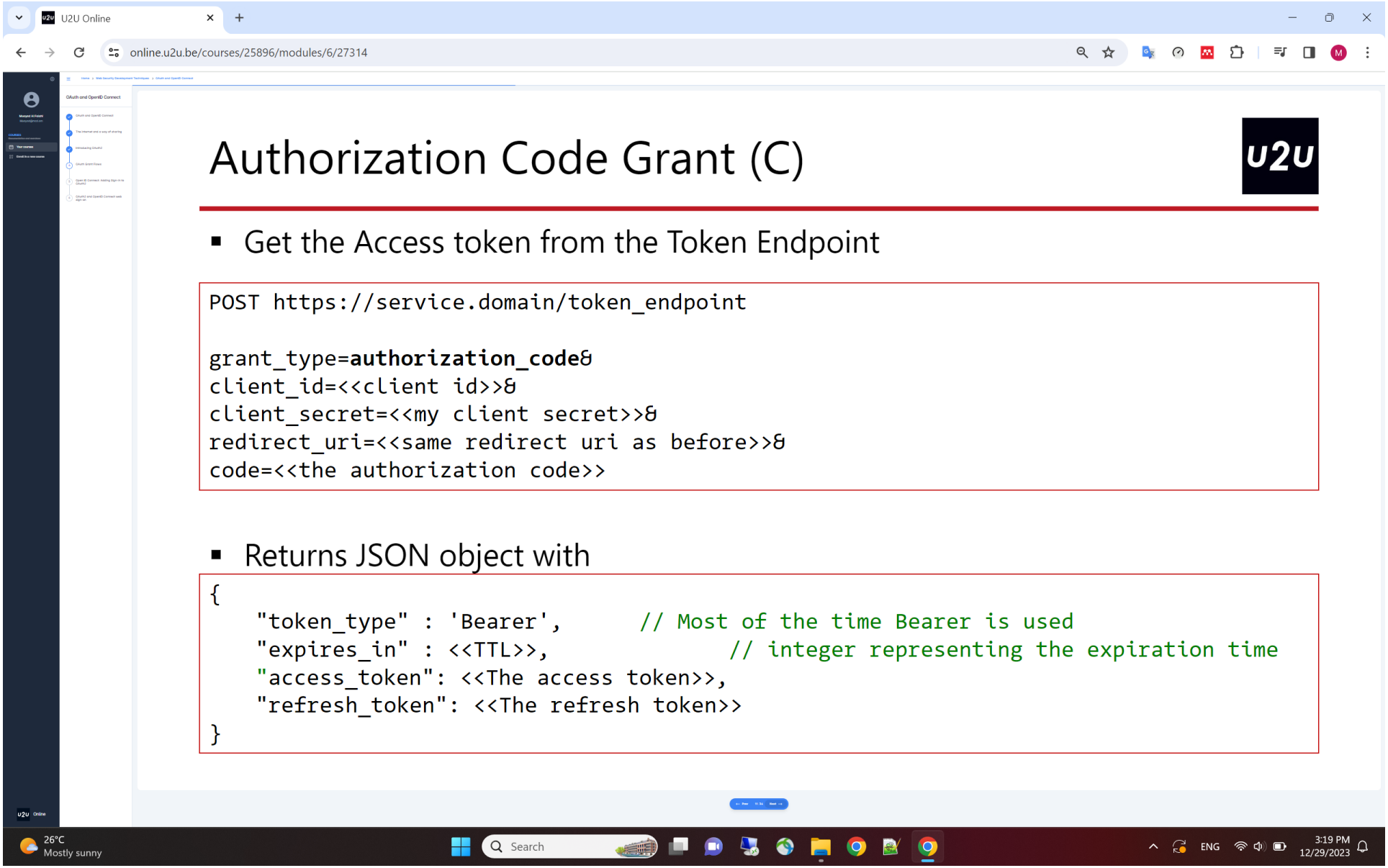

U2U Online
online.u2u.be/courses/25896/modules/6/27314
Simplified OAuth2 flow between web applications
U2U
A
B
Browser
Authorization Server
1. Please do something
2. Redirect to AS
3. "Can I?" get code
4. Code
5. Code + App Credentials
6.
7.
Authorization
26°C
Mostly sunny
Search
ENG
3:19 PM
12/29/2023

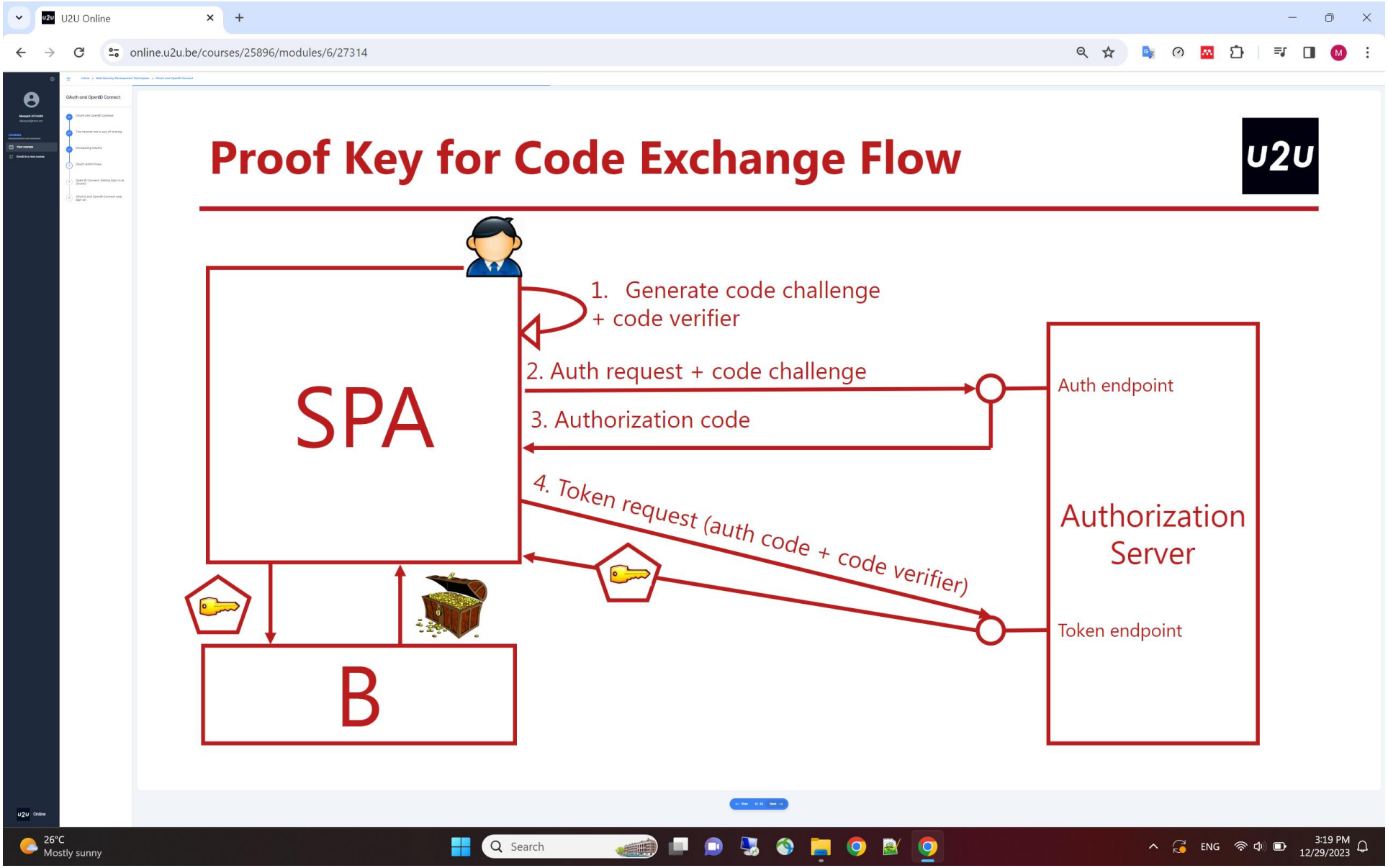

U2U Online
online.u2u.be/courses/25896/modules/6/27314
Most common OAuth Grant Flows
U2U
Authorization Code Grant
Useful for web app executing on the server and natively installed apps
Proof Key for Code Exchange
Improved Security for Public Clients (JavaScript and Native applications)
Resource owner credentials grant
Only useful if the client app is absolutely trusted with the user credentials
Client credentials grant
Useful for unattended apps like services, server to server communication,...
Refresh token grant
Used to refresh an access token when it expires
26°C
Mostly sunny
Search
ENG
3:19 PM
12/29/2023


U2U Online
online.u2u.be/courses/25896/modules/6/27314
Authorization code flow
u2u
A
B
Native
Authorization Server
1. Please do something
2. Redirect to AS
3. Auth code?
4. Auth Code
5. Auth Code + Credentials
6.
7.
Authorization
26°C
Mostly sunny
Search
ENG
3:19 PM
12/29/2023


U2U Online
online.u2u.be/courses/25896/modules/6/27314
Authorization Code Grant (A)
u2u
Redirect user to Authorization Endpoint
keyword
https://service.domain/authorization_endpoint?
response_type=code&
client_id=<<my client id>>&
redirect_uri=https://my.local.domain/resource&
scope=api,profile,…&
state=<<CSRF Token>>
optional (registered url will be taken)
Depends on the application
optional (CSRF token stored in User Session state and checked in web app)
26°C
Mostly sunny
Search
ENG
3:19 PM
12/29/2023

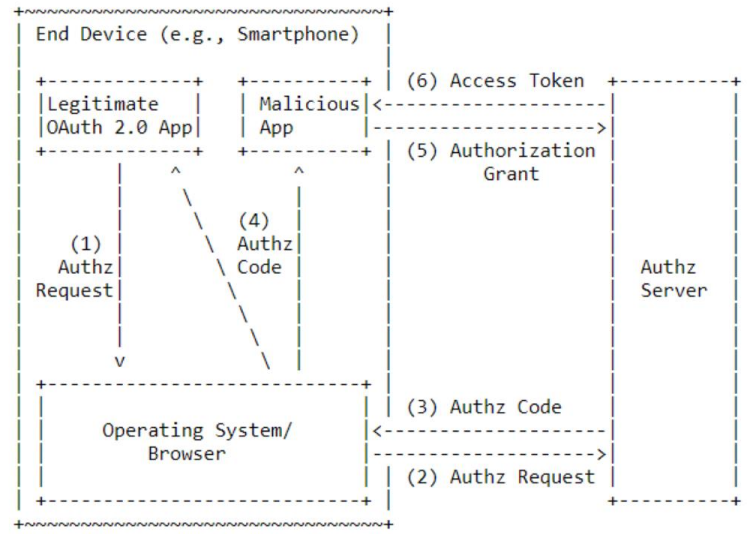

U2U Online
online.u2u.be/courses/25896/modules/6/27314
Authorization Code Grant (B)
U2U
Redirect user back to Web App
Code to be used to fetch access tokens
https://my.local.domain/resource?
code=<<the authorization code>>&
state=<<same CSRF Token>>
CSRF token returned from Authorization Server to be checked in Web App
26°C
Mostly sunny
Search
ENG
3:19 PM
12/29/2023

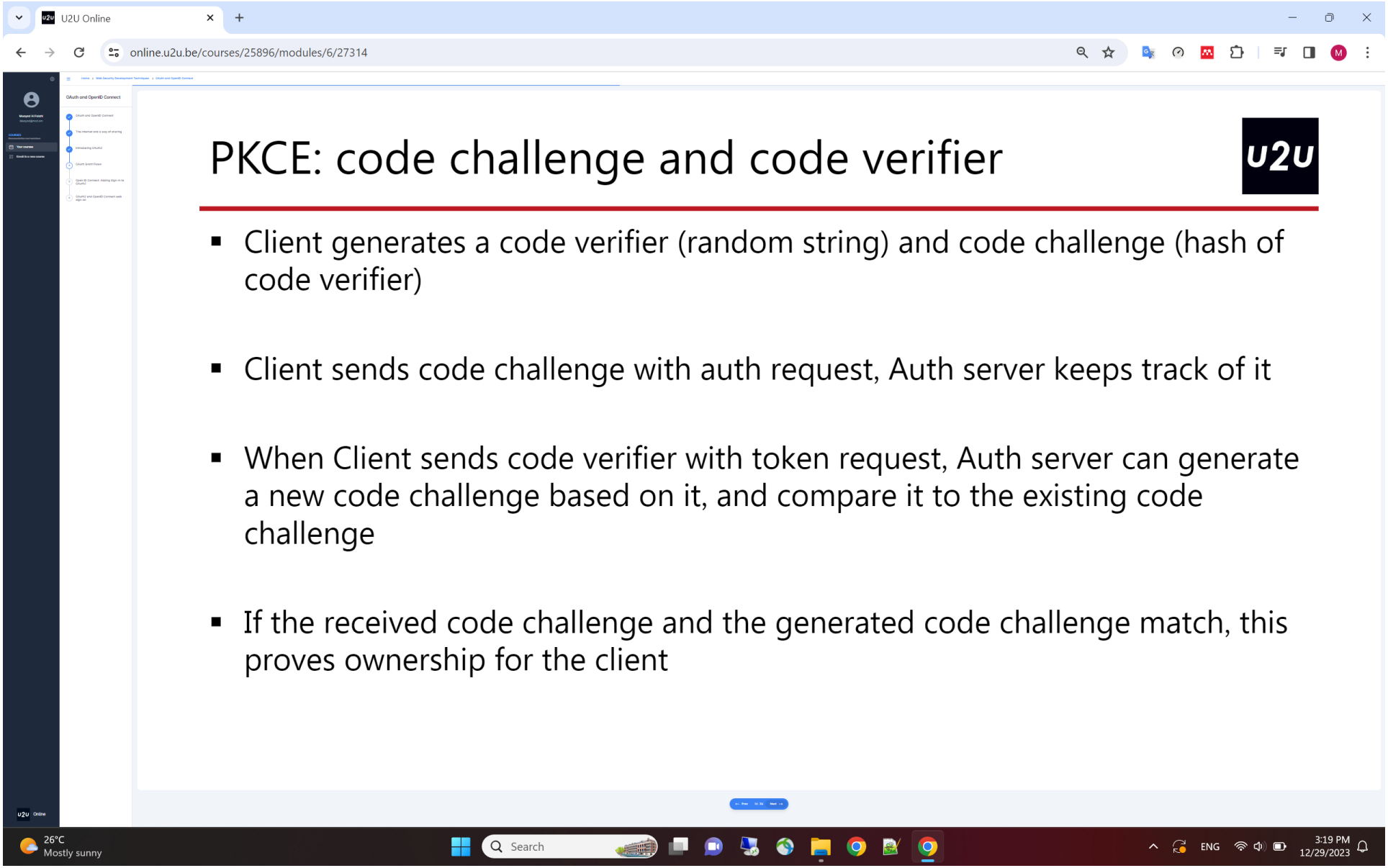

U2U Online
online.u2u.be/courses/25896/modules/6/27314
Authorization Code Grant (C)
u2u
Get the Access token from the Token Endpoint
POST https://service.domain/token_endpoint
grant_type=authorization_code&
client_id=<<client id>>&
client_secret=<<my client secret>>&
redirect_uri=<<same redirect uri as before>>&
code=<<the authorization code>>
Returns JSON object with
{
"token_type" : 'Bearer', // Most of the time Bearer is used
"expires_in" : <<TTL>>, // integer representing the expiration time
"access_token": <<The access token>>,
"refresh_token": <<The refresh token>>
}
26°C
Mostly sunny
Search
ENG
3:19 PM
12/29/2023

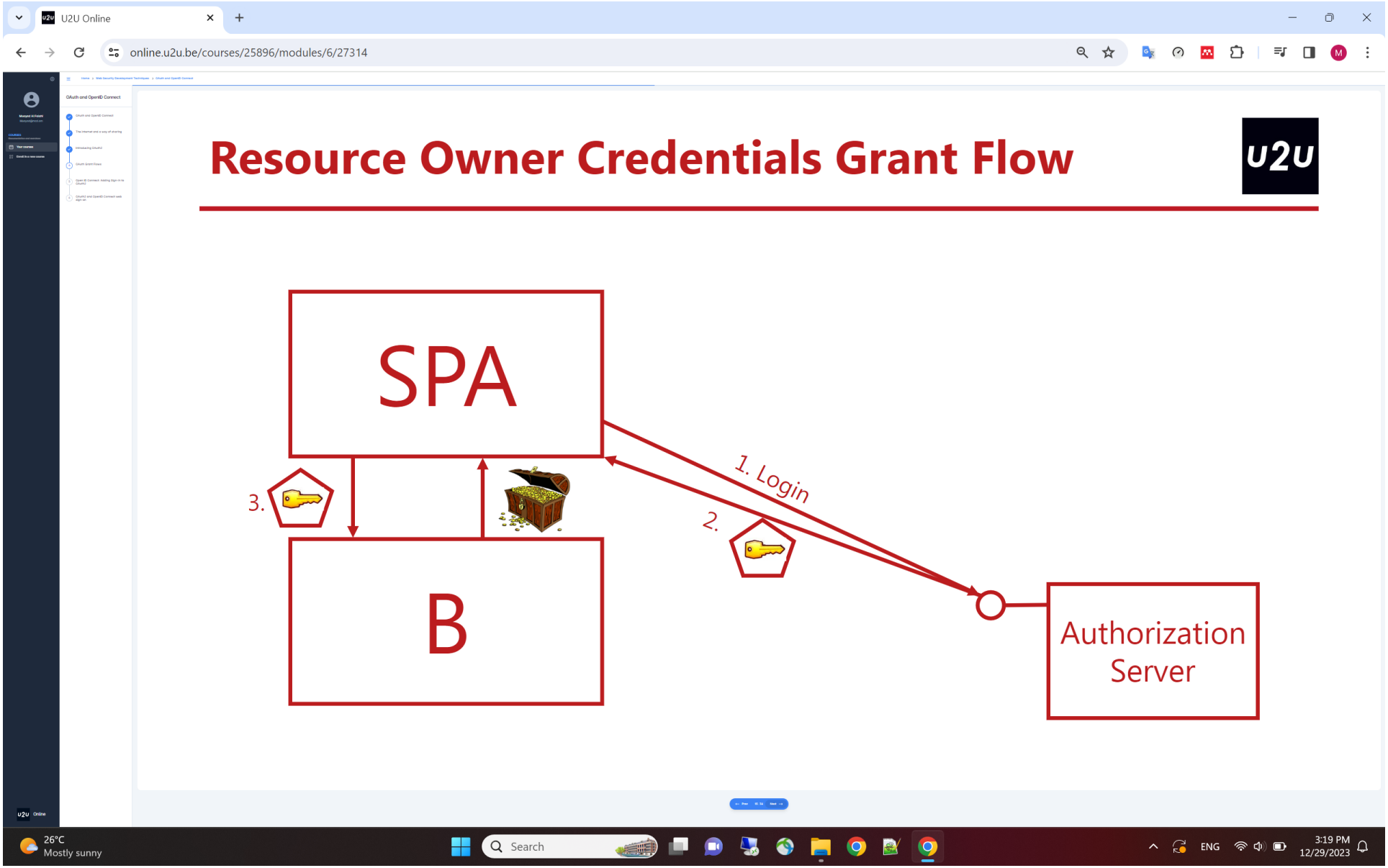

U2U Online
online.u2u.be/courses/25896/modules/6/27314
Proof Key for Code Exchange Flow
u2u
SPA
B
1. Generate code challenge
+ code verifier
2. Auth request + code challenge
3. Authorization code
4. Token request (auth code + code verifier)
Auth endpoint
Authorization Server
Token endpoint
26°C
Mostly sunny
Search
ENG
3:19 PM
12/29/2023

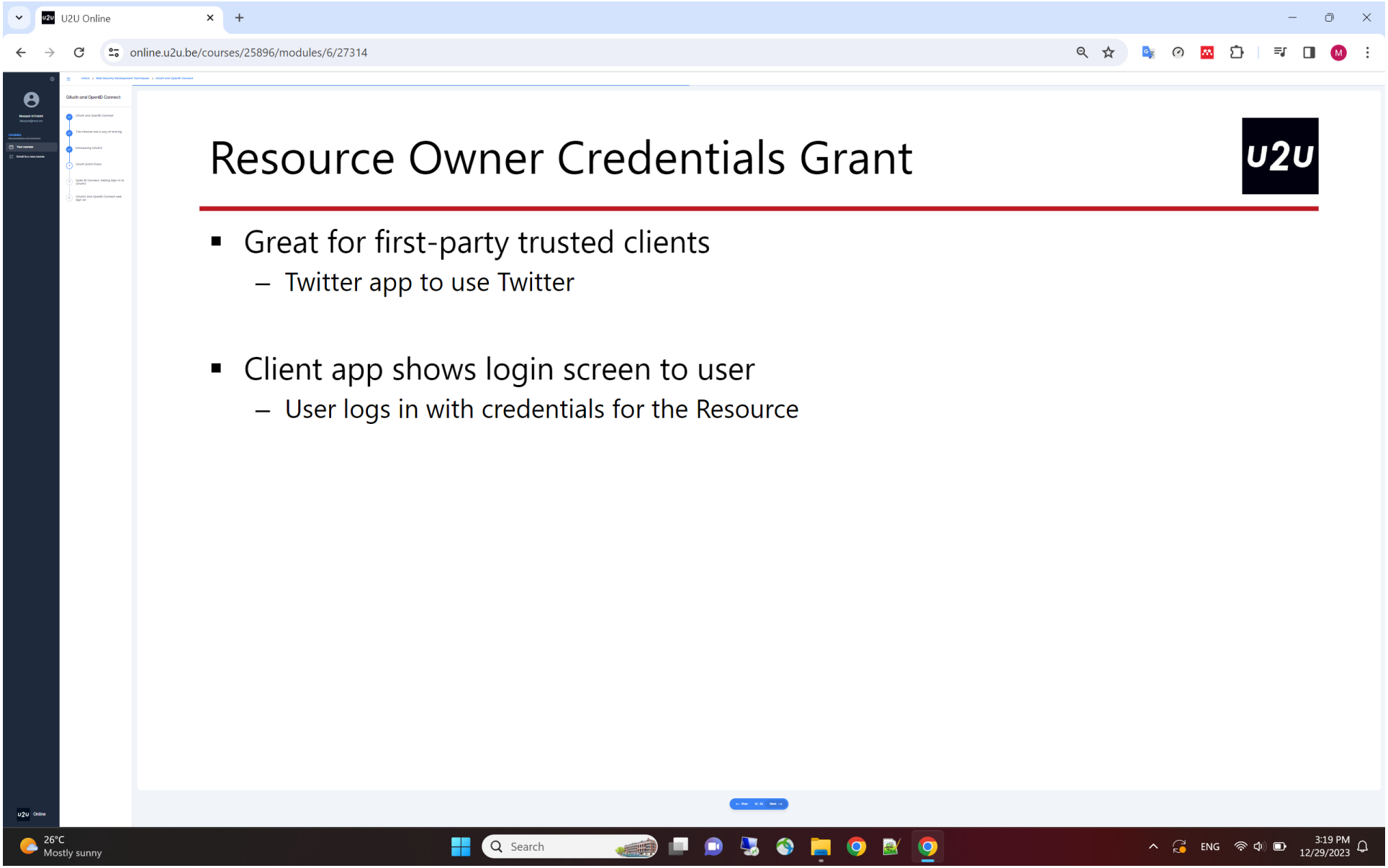
PKCE Flow

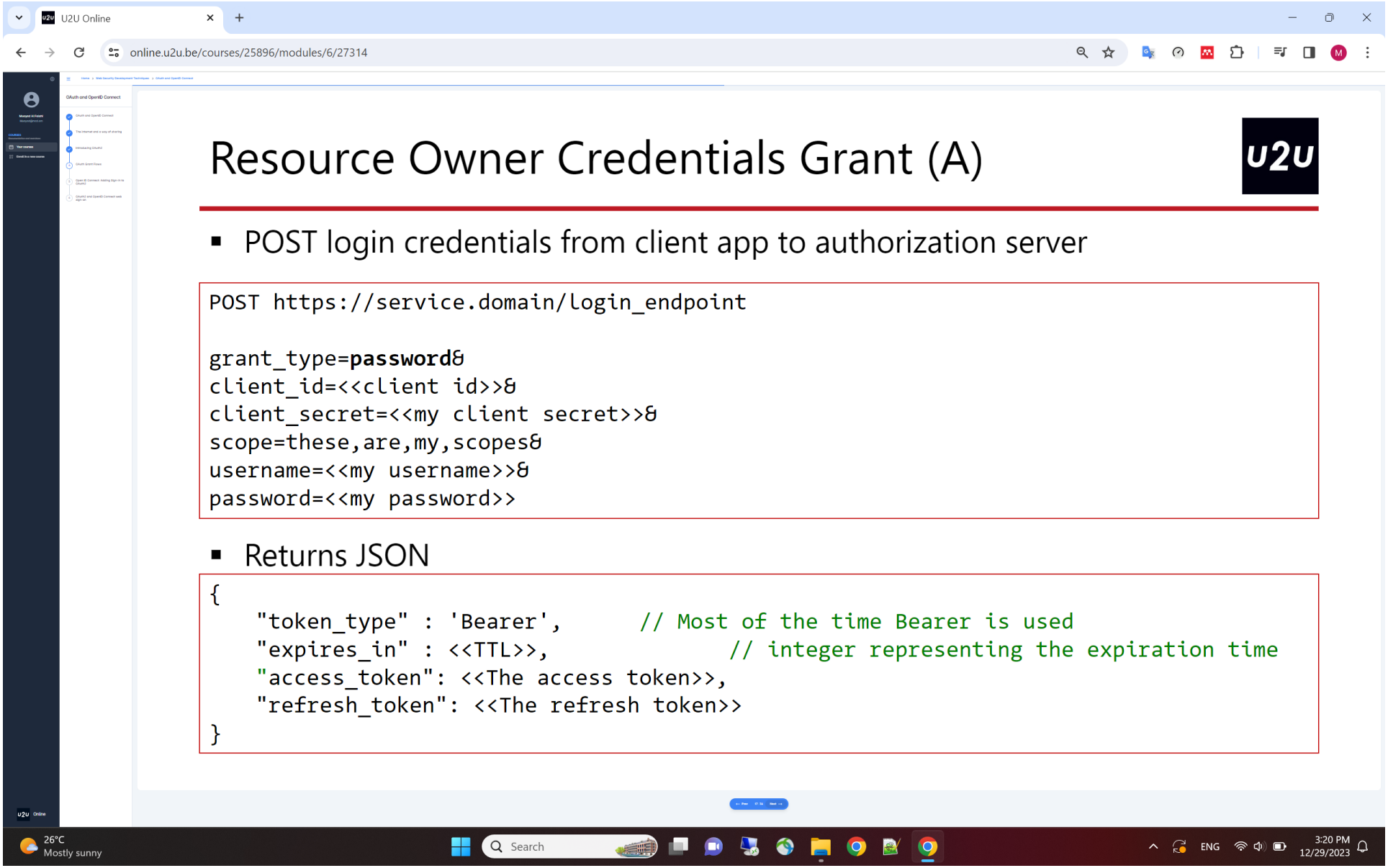
- For public clients, Authorization Code Grant is vulnerable to an authorization code interception attack
- PKCE uses a code challenge and code verifier to prevent authorization code interception attacks

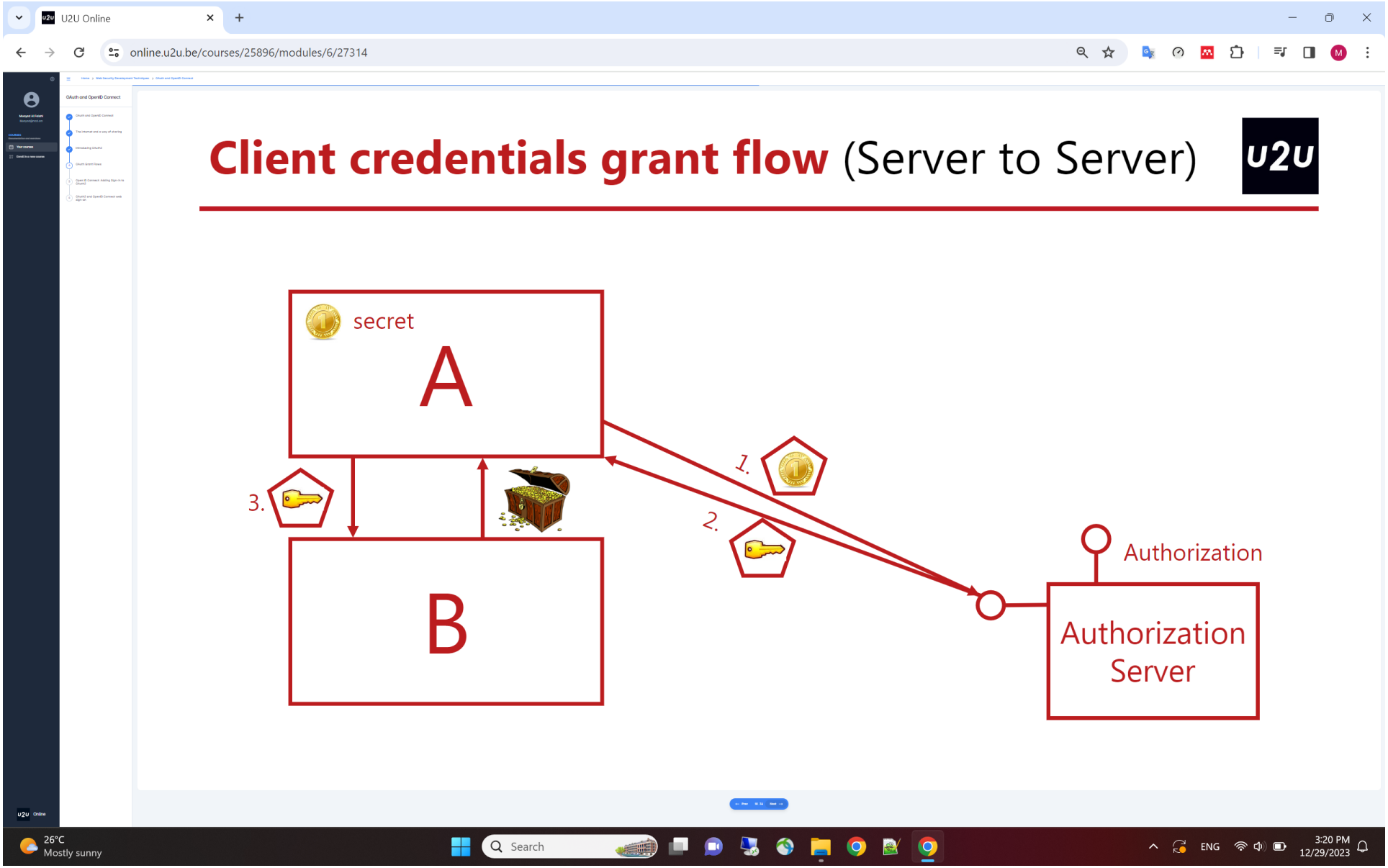


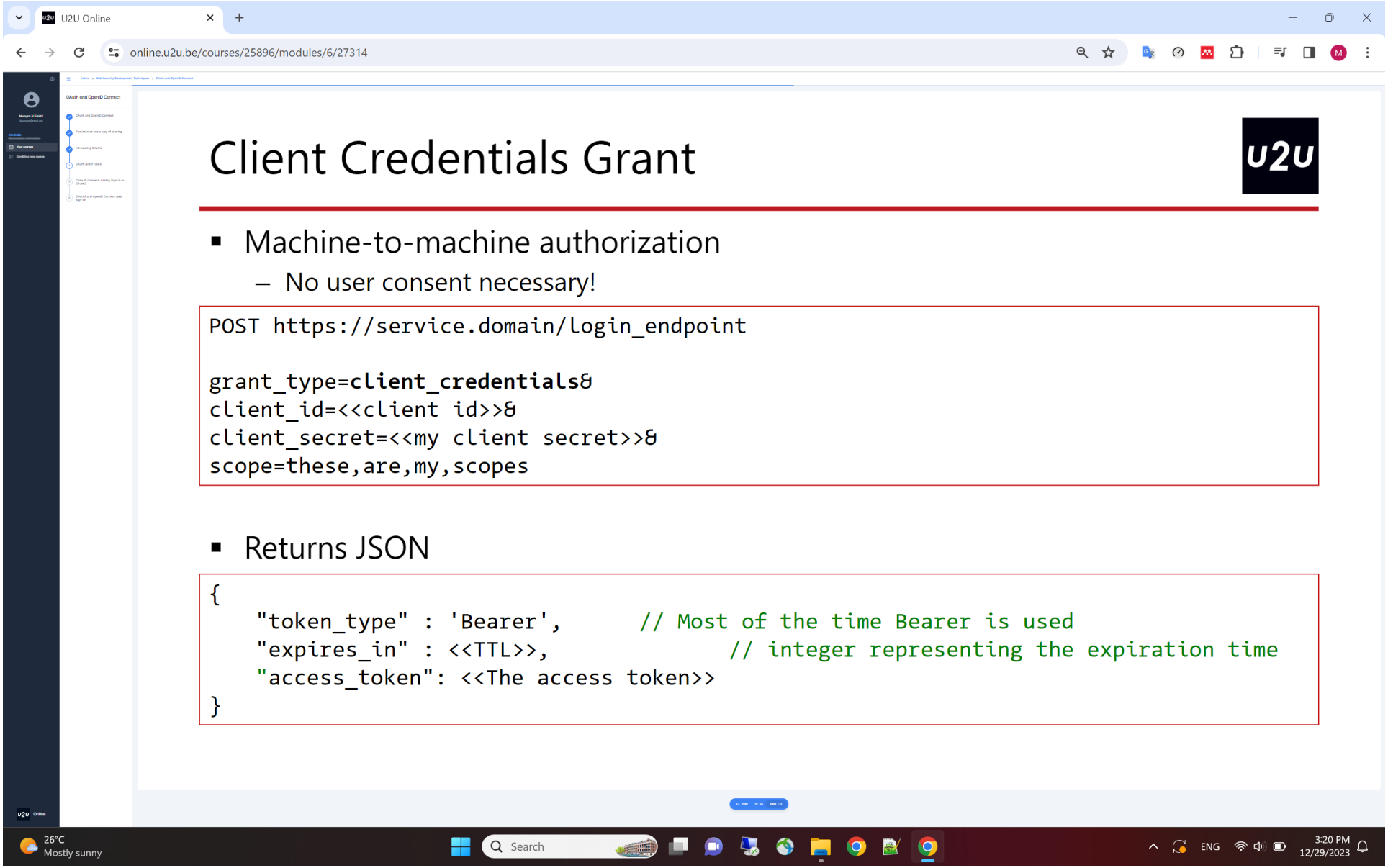

U2U Online
online.u2u.be/courses/25896/modules/6/27314
PKCE: code challenge and code verifier
U2U
Client generates a code verifier (random string) and code challenge (hash of code verifier)
Client sends code challenge with auth request, Auth server keeps track of it
When Client sends code verifier with token request, Auth server can generate a new code challenge based on it, and compare it to the existing code challenge
If the received code challenge and the generated code challenge match, this proves ownership for the client
26°C
Mostly sunny
Search
ENG
3:19 PM
12/29/2023

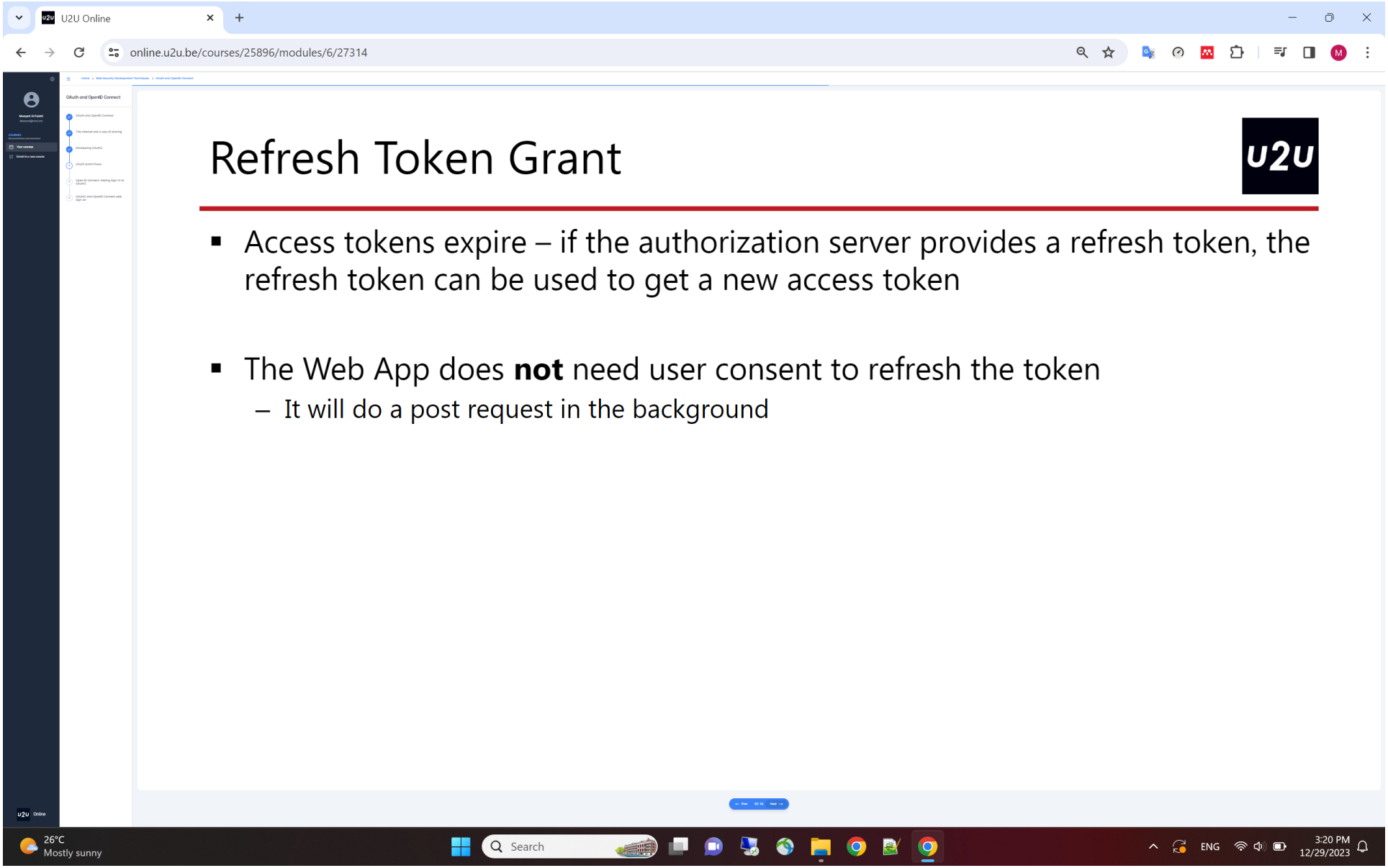

U2U Online
online.u2u.be/courses/25896/modules/6/27314
Resource Owner Credentials Grant Flow
u2u
SPA
B
3.
1. Login
2.
Authorization Server
26°C
Mostly sunny
Search
ENG
3:19 PM
12/29/2023

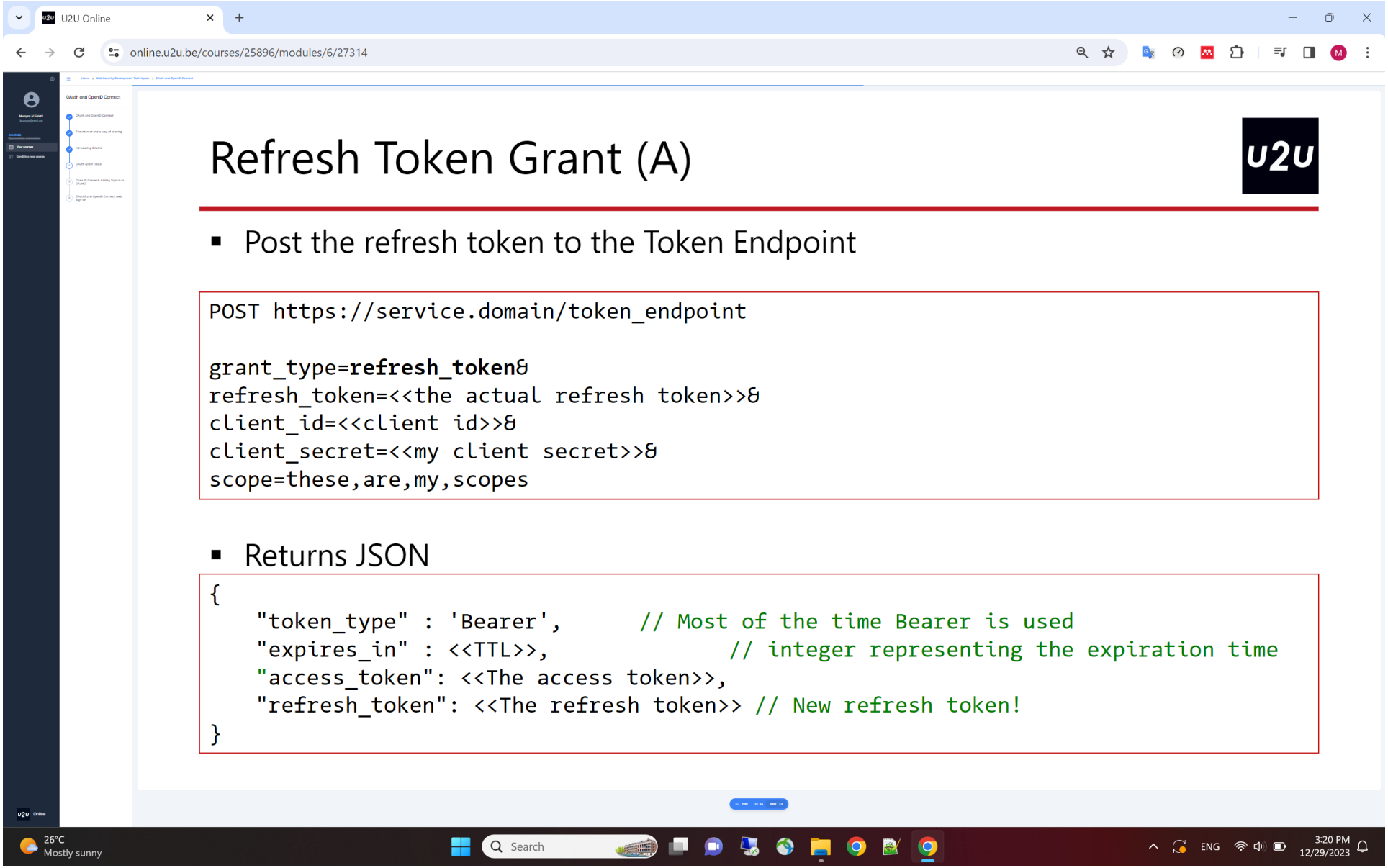

U2U Online
online.u2u.be/courses/25896/modules/6/27314
Resource Owner Credentials Grant
u2u
Great for first-party trusted clients
Twitter app to use Twitter
Client app shows login screen to user
User logs in with credentials for the Resource
26°C
Mostly sunny
Search
ENG
3:19 PM
12/29/2023

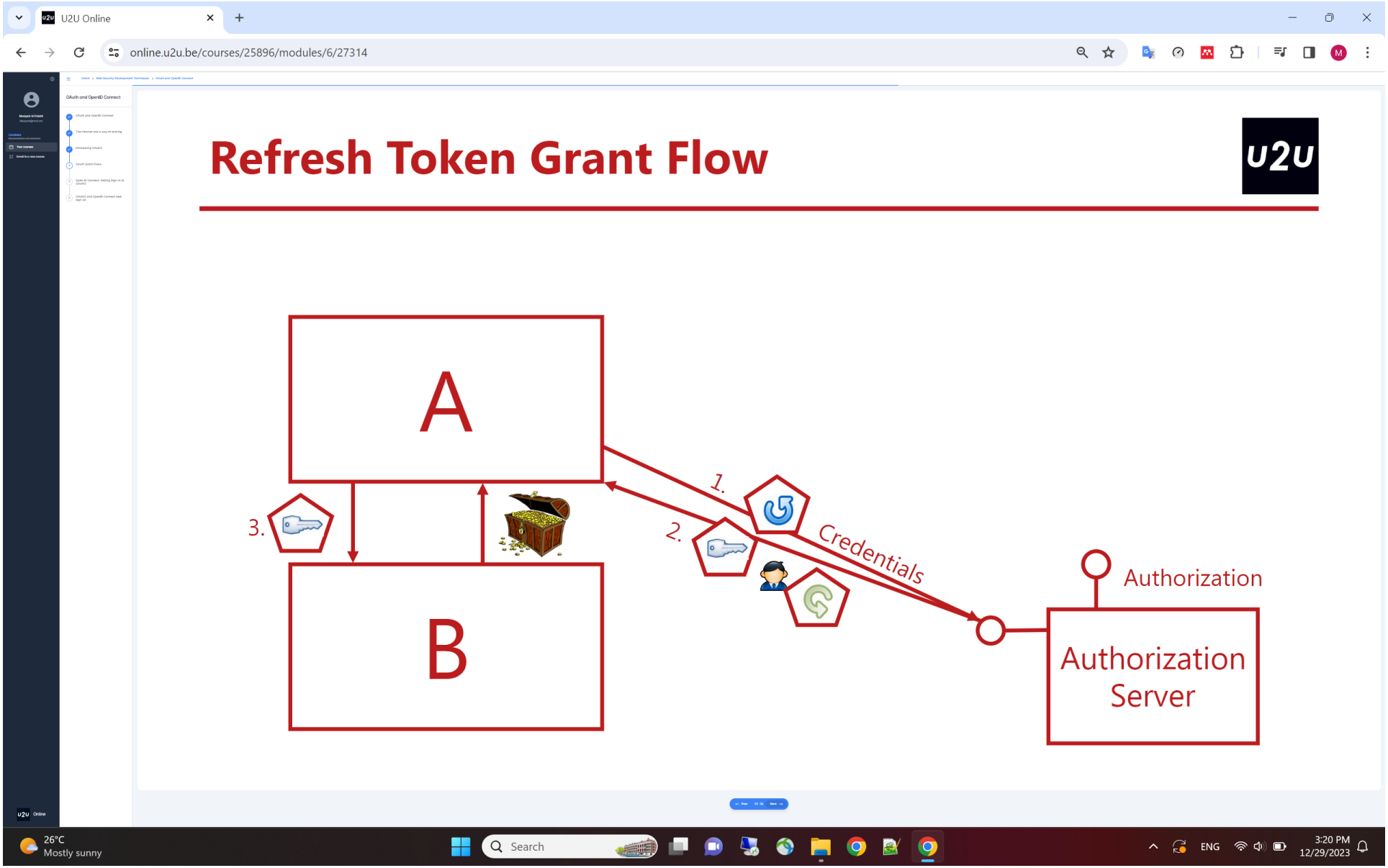

U2U Online
online.u2u.be/courses/25896/modules/6/27314
Resource Owner Credentials Grant (A)
U2U
POST login credentials from client app to authorization server
POST https://service.domain/login_endpoint
grant_type=password&
client_id=<<client id>>&
client_secret=<<my client secret>>&
scope=these,are,my,scopes&
username=<<my username>>&
password=<<my password>>
Returns JSON
{
"token_type" : 'Bearer', // Most of the time Bearer is used
"expires_in" : <<TTL>>, // integer representing the expiration time
"access_token": <<The access token>>,
"refresh_token": <<The refresh token>>
}
26°C
Mostly sunny
Search
ENG
3:20 PM
12/29/2023

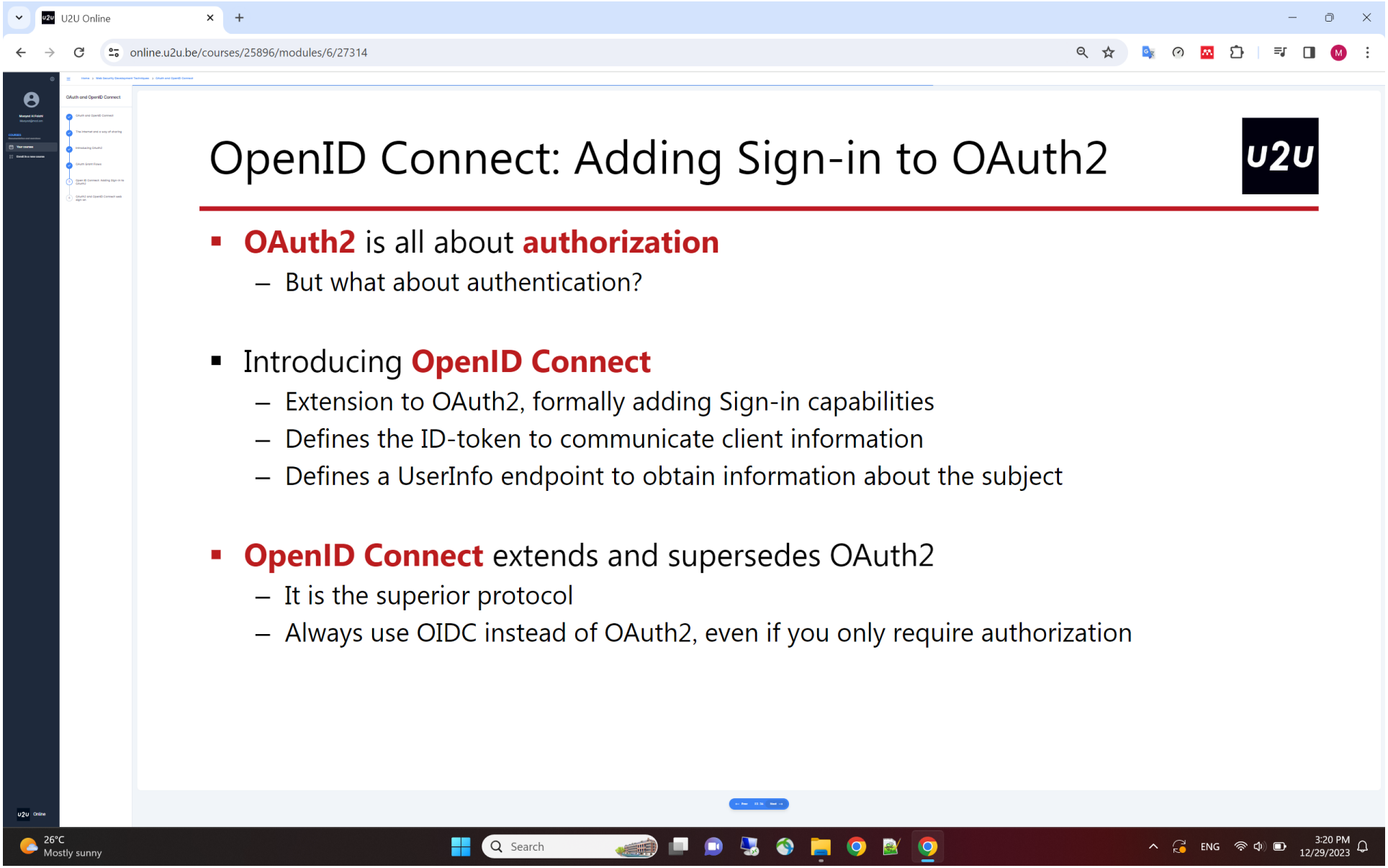

U2U Online
online.u2u.be/courses/25896/modules/6/27314
Client credentials grant flow (Server to Server)
u2u
secret
A
B
1.
2.
3.
Authorization
Authorization Server
26°C
Mostly sunny
Search
ENG
3:20 PM
12/29/2023

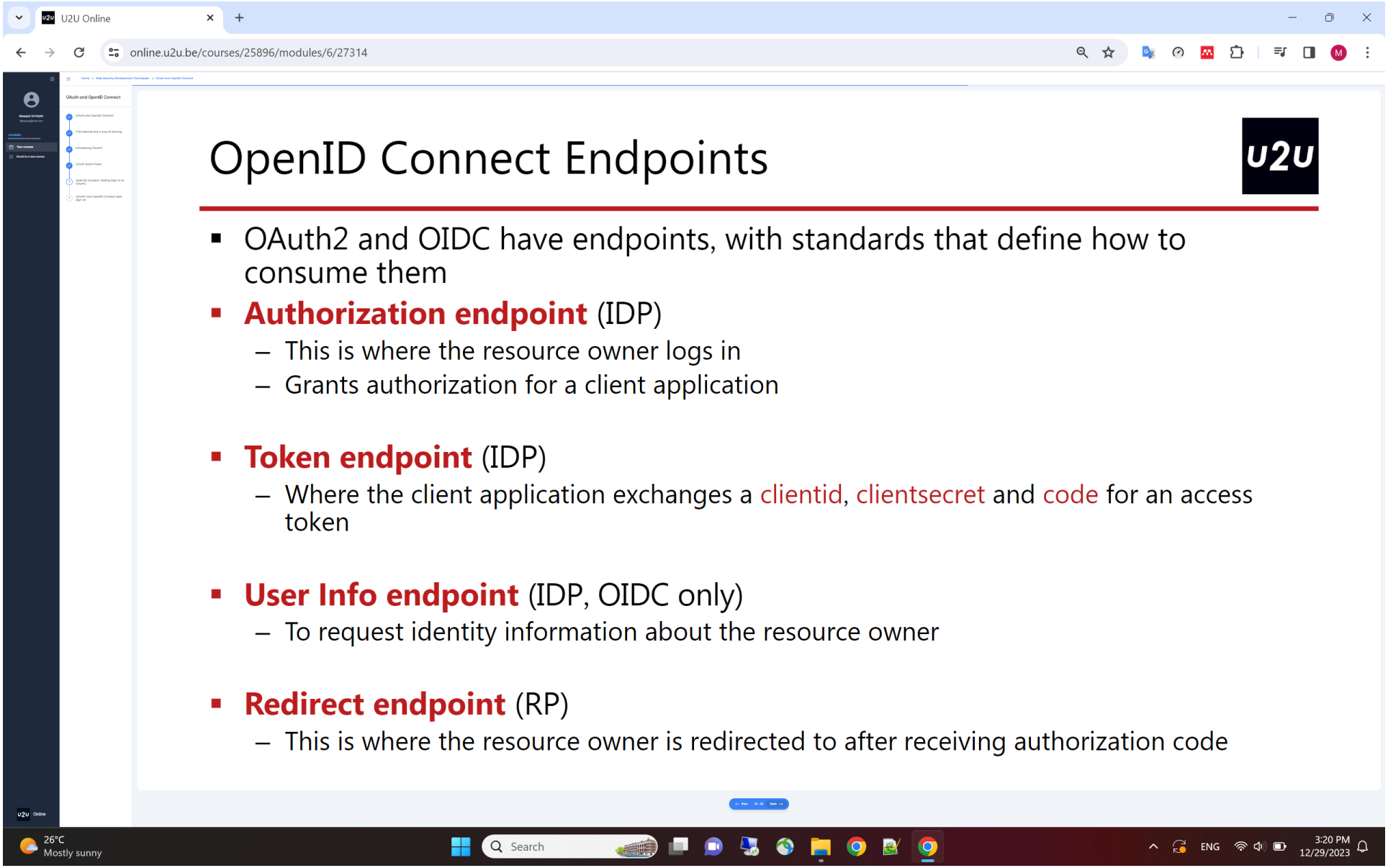

U2U Online
online.u2u.be/courses/25896/modules/6/27314
Client Credentials Grant
U2U
Machine-to-machine authorization
No user consent necessary!
POST https://service.domain/login_endpoint
grant_type=client_credentials&
client_id=<<client id>>&
client_secret=<<my client secret>>&
scope=these,are,my,scopes
Returns JSON
{
"token_type" : 'Bearer', // Most of the time Bearer is used
"expires_in" : <<TTL>>, // integer representing the expiration time
"access_token": <<The access token>>
}
26°C
Mostly sunny
Search
ENG
3:20 PM
12/29/2023


U2U Online
online.u2u.be/courses/25896/modules/6/27314
Refresh Token Grant
u2u
Access tokens expire – if the authorization server provides a refresh token, the refresh token can be used to get a new access token
The Web App does **not** need user consent to refresh the token
It will do a post request in the background
26°C
Mostly sunny
Search
ENG
3:20 PM
12/29/2023


U2U Online
online.u2u.be/courses/25896/modules/6/27314
Refresh Token Grant (A)
U2U
Post the refresh token to the Token Endpoint
POST https://service.domain/token_endpoint
grant_type=refresh_token&
refresh_token=<<the actual refresh token>>&
client_id=<<client id>>&
client_secret=<<my client secret>>&
scope=these,are,my,scopes
Returns JSON
{
"token_type" : 'Bearer', // Most of the time Bearer is used
"expires_in" : <<TTL>>, // integer representing the expiration time
"access_token": <<The access token>>,
"refresh_token": <<The refresh token>> // New refresh token!
}
26°C
Mostly sunny
Search
ENG
3:20 PM
12/29/2023


U2U Online
online.u2u.be/courses/25896/modules/6/27314
Refresh Token Grant Flow
u2u
A
B
1.
2.
3.
Credentials
Authorization
Authorization Server
26°C
Mostly sunny
Search
ENG
3:20 PM
12/29/2023


U2U Online
online.u2u.be/courses/25896/modules/6/27314
OpenID Connect: Adding Sign-in to OAuth2
u2u
OAuth2 is all about authorization
But what about authentication?
Introducing OpenID Connect
Extension to OAuth2, formally adding Sign-in capabilities
Defines the ID-token to communicate client information
Defines a UserInfo endpoint to obtain information about the subject
OpenID Connect extends and supersedes OAuth2
It is the superior protocol
Always use OIDC instead of OAuth2, even if you only require authorization
26°C
Mostly sunny
Search
ENG
3:20 PM
12/29/2023


U2U Online
online.u2u.be/courses/25896/modules/6/27314
OpenID Connect Endpoints
u2u
OAuth2 and OIDC have endpoints, with standards that define how to consume them
Authorization endpoint (IDP)
This is where the resource owner logs in
Grants authorization for a client application
Token endpoint (IDP)
Where the client application exchanges a clientid, clientsecret and code for an access token
User Info endpoint (IDP, OIDC only)
To request identity information about the resource owner
Redirect endpoint (RP)
This is where the resource owner is redirected to after receiving authorization code
26°C
Mostly sunny
Search
ENG
3:20 PM
12/29/2023

U2U Online

online.u2u.be/courses/25896/modules/6/27314

OpenID Connect Flows

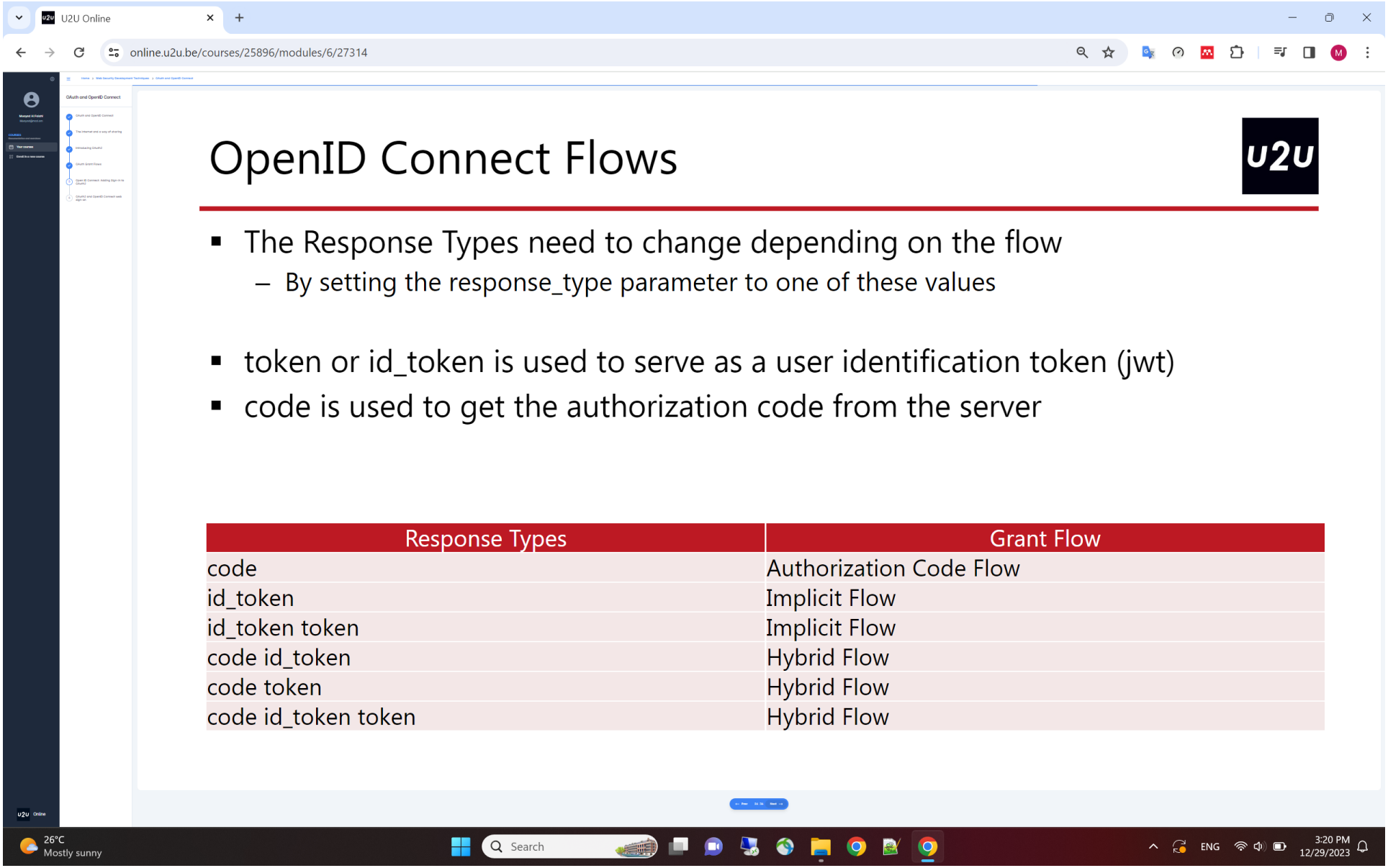
- **Authorization Code Flow**
  - Authorization Code from Authorization Endpoint
  - Tokens come from Token Endpoint
  - For confidential clients
  - Give long-lived access
- **Implicit Flow**
  - Tokens come from authorization endpoint
  - For public clients
  - No long-lived access
- **Hybrid Flow**
  - Authorization Code from Authorization Endpoint
  - Tokens come from Authorization & Token Endpoint
  - For confidential clients
  - Give long-lived access

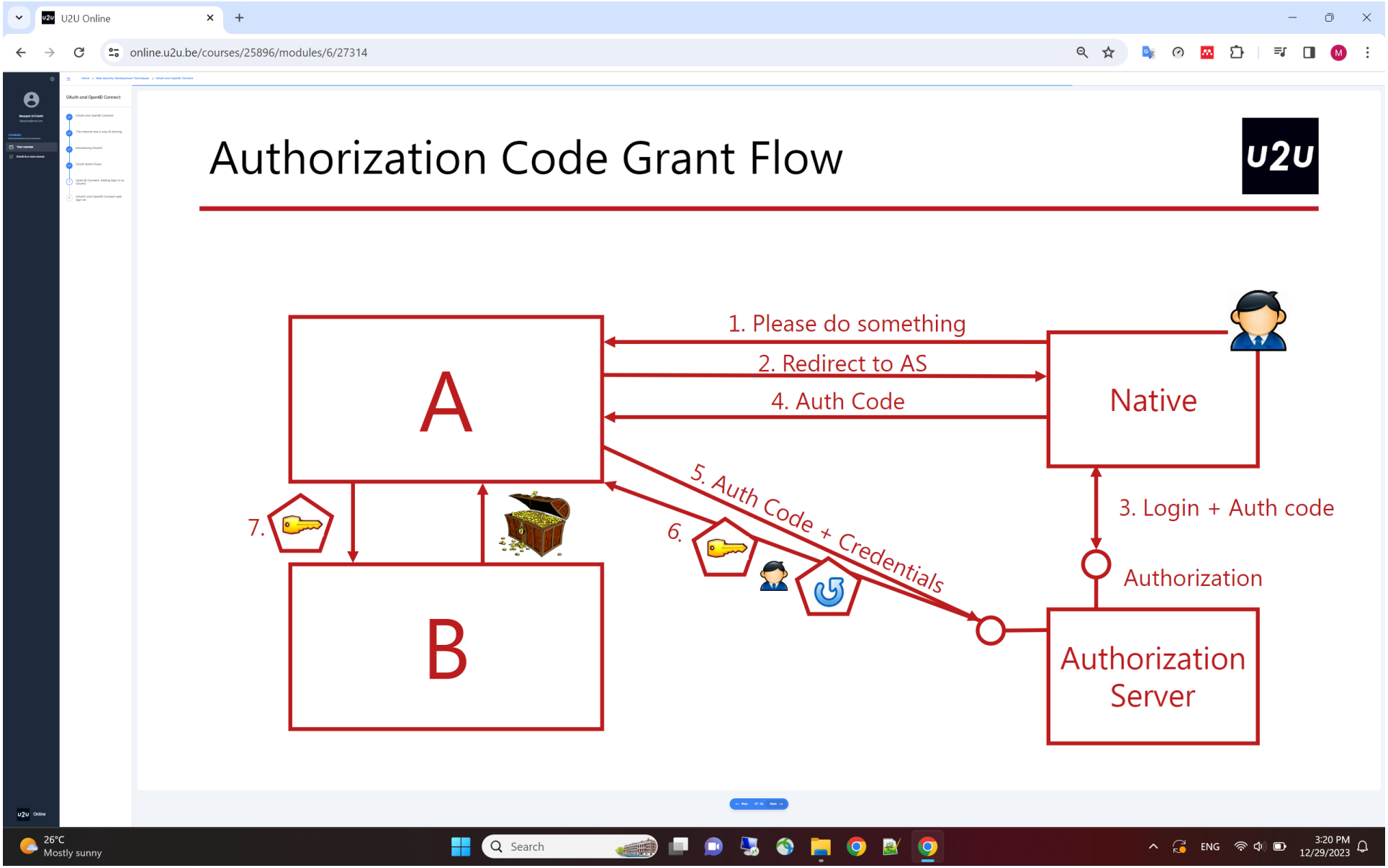
26°C Mostly sunny

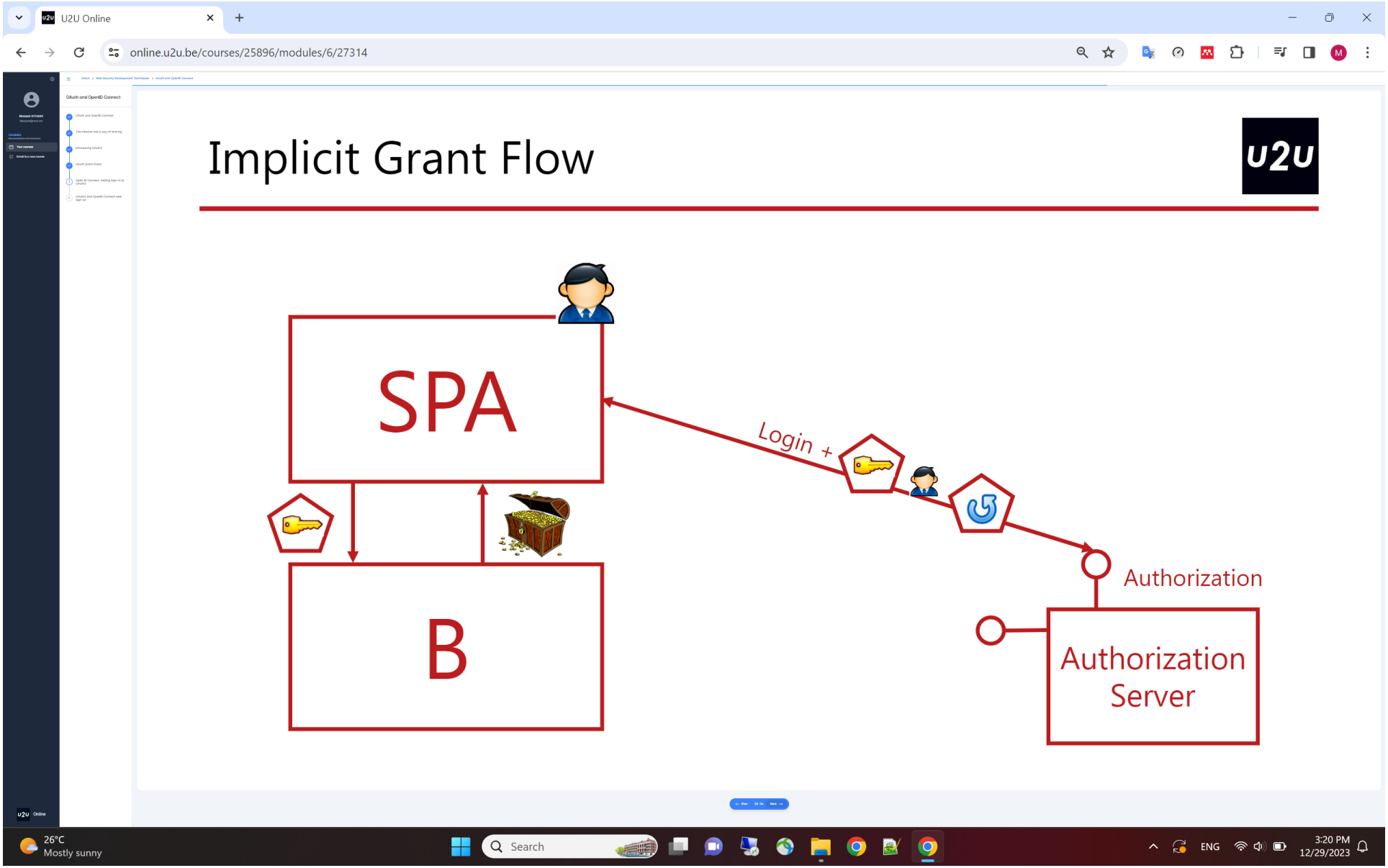
Search

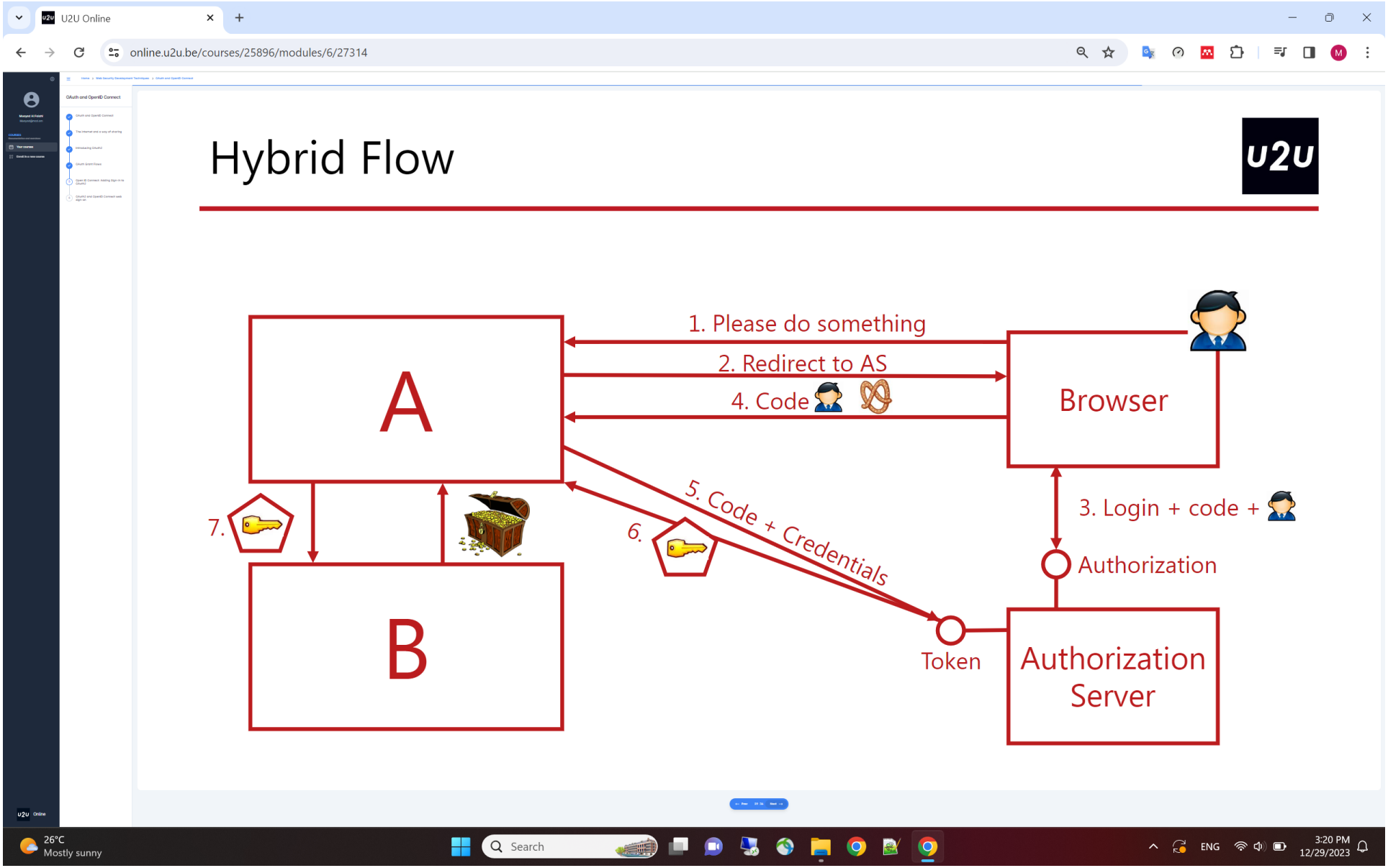
ENG

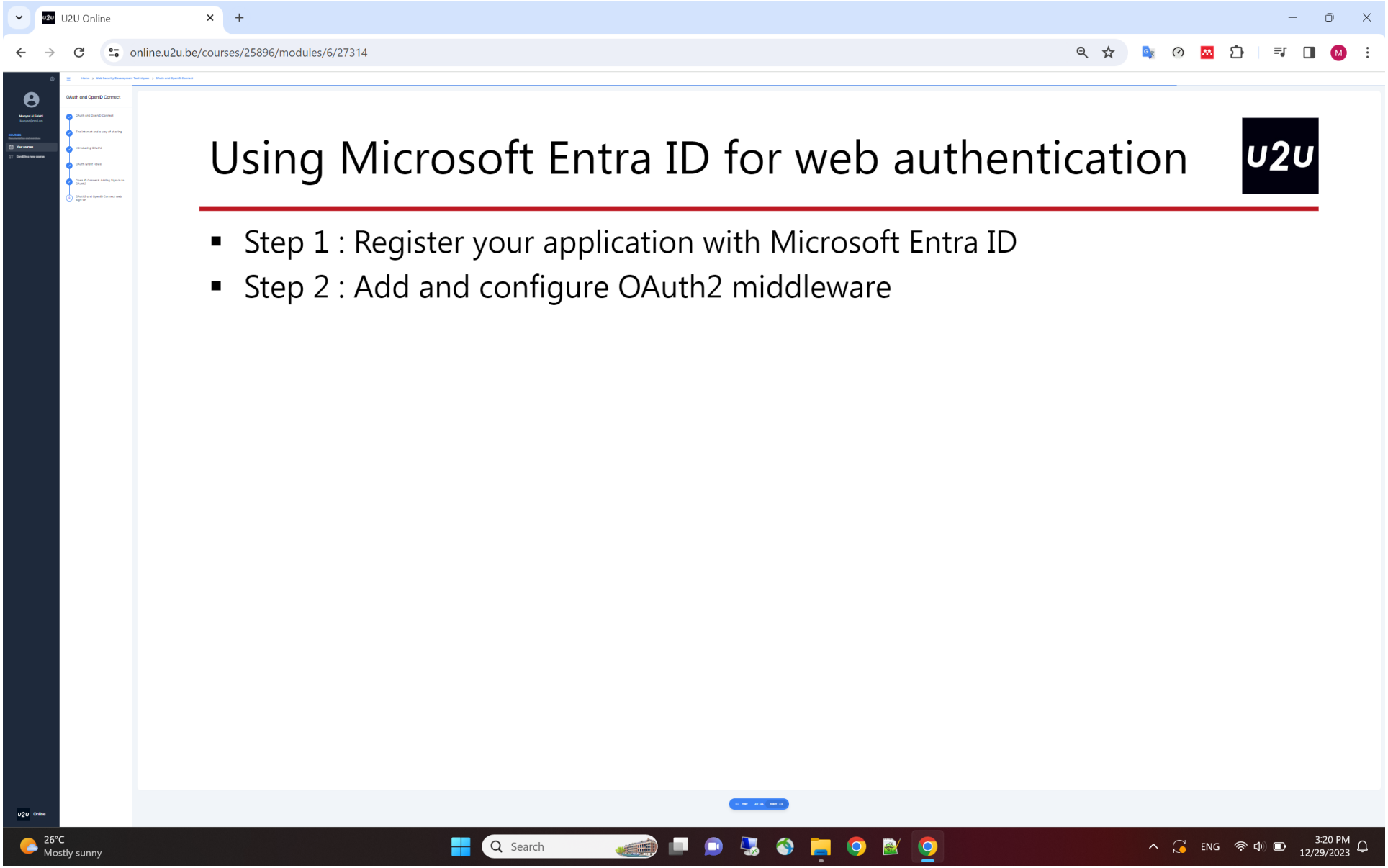
3:20 PM 12/29/2023

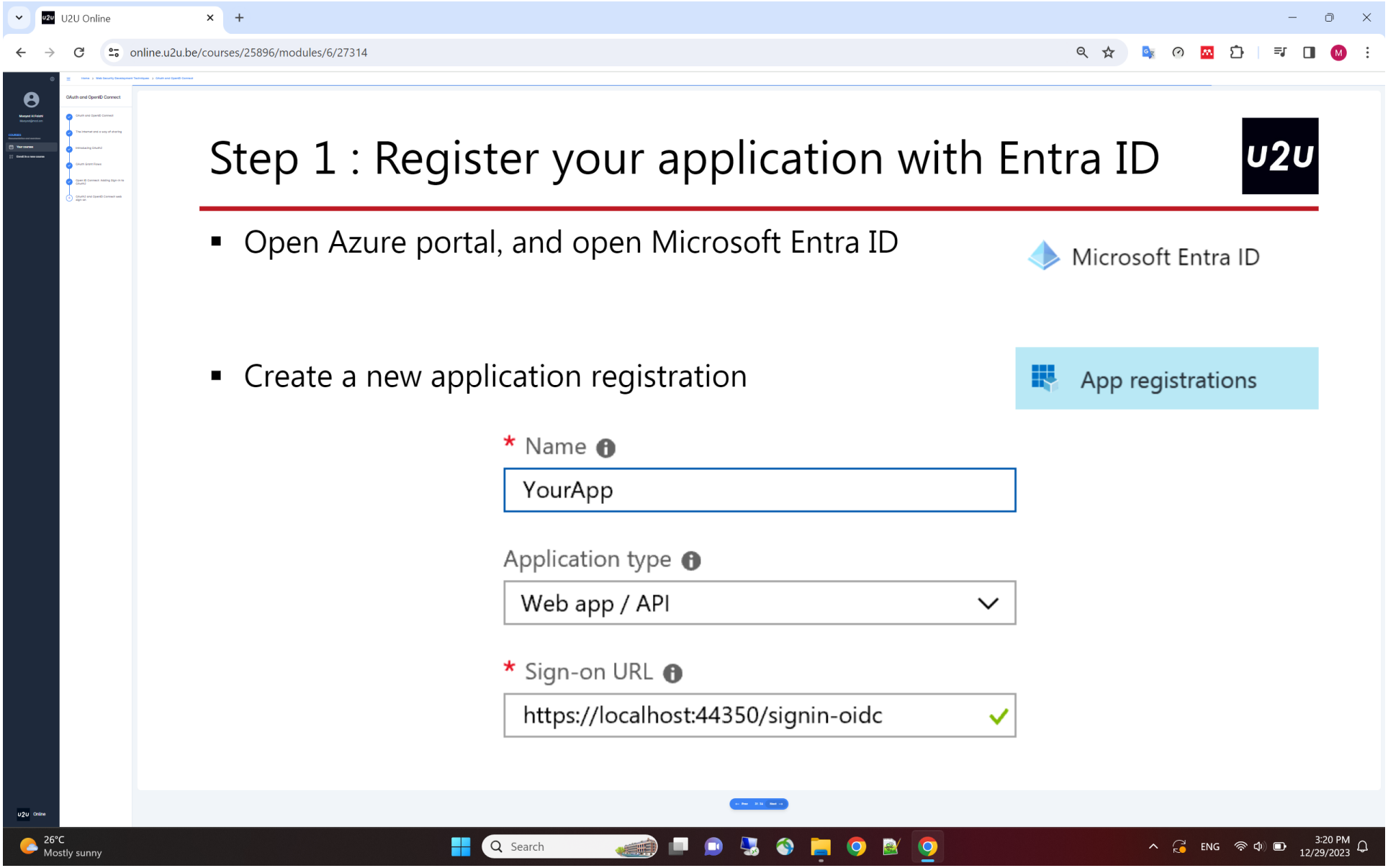

U2U Online
online.u2u.be/courses/25896/modules/6/27314
OpenID Connect Flows
u2u
The Response Types need to change depending on the flow
By setting the response_type parameter to one of these values
token or id_token is used to serve as a user identification token (jwt)
code is used to get the authorization code from the server
Response Types
Grant Flow
code
Authorization Code Flow
id_token
Implicit Flow
id_token token
Implicit Flow
code id_token
Hybrid Flow
code token
Hybrid Flow
code id_token token
Hybrid Flow
26°C
Mostly sunny
Search
ENG
3:20 PM
12/29/2023

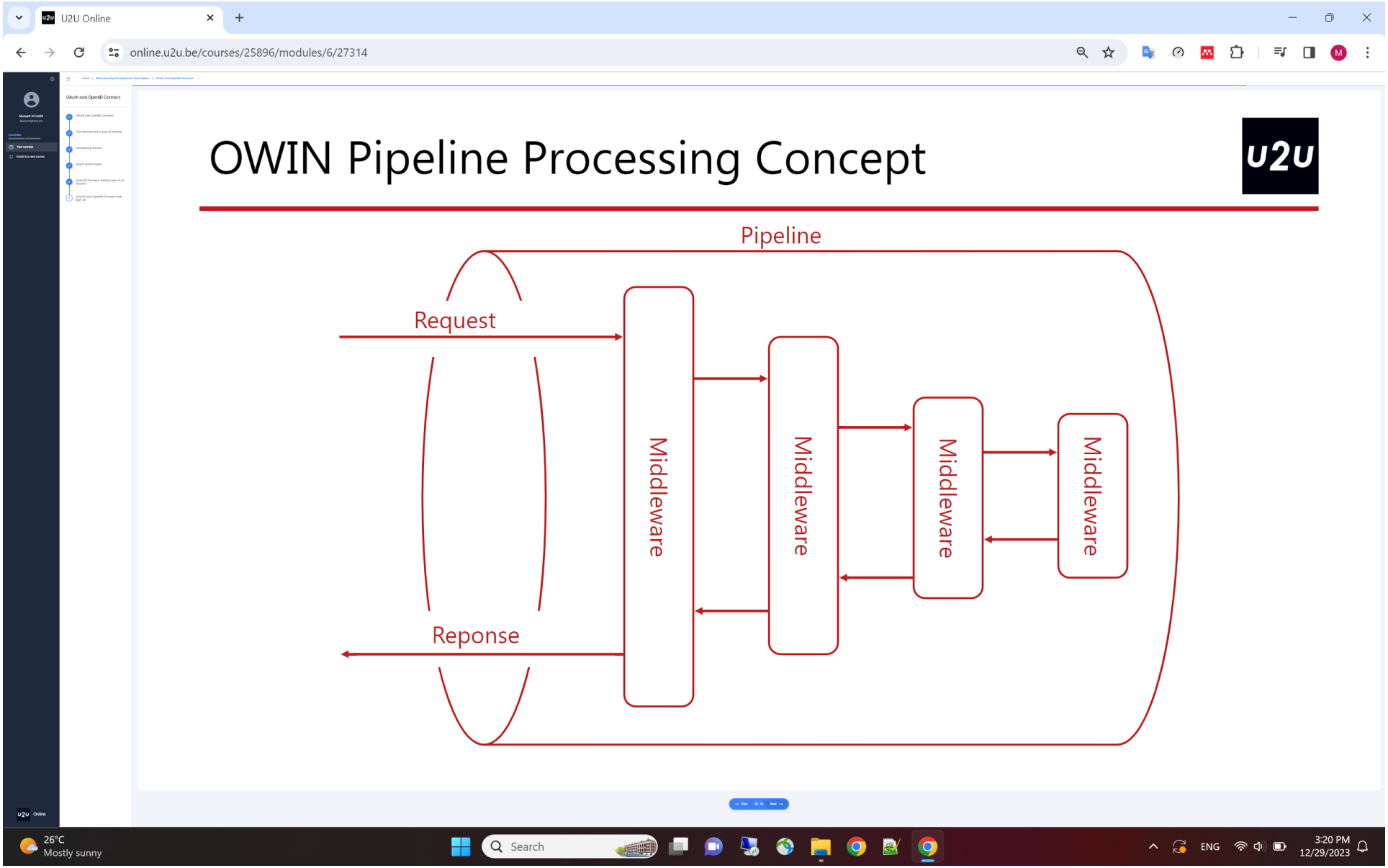

U2U Online
online.u2u.be/courses/25896/modules/6/27314
Authorization Code Grant Flow
u2u
A
B
Native
Authorization Server
1. Please do something
2. Redirect to AS
3. Login + Auth code
4. Auth Code
5. Auth Code + Credentials
6.
7.
Authorization
26°C
Mostly sunny
Search
ENG
3:20 PM
12/29/2023

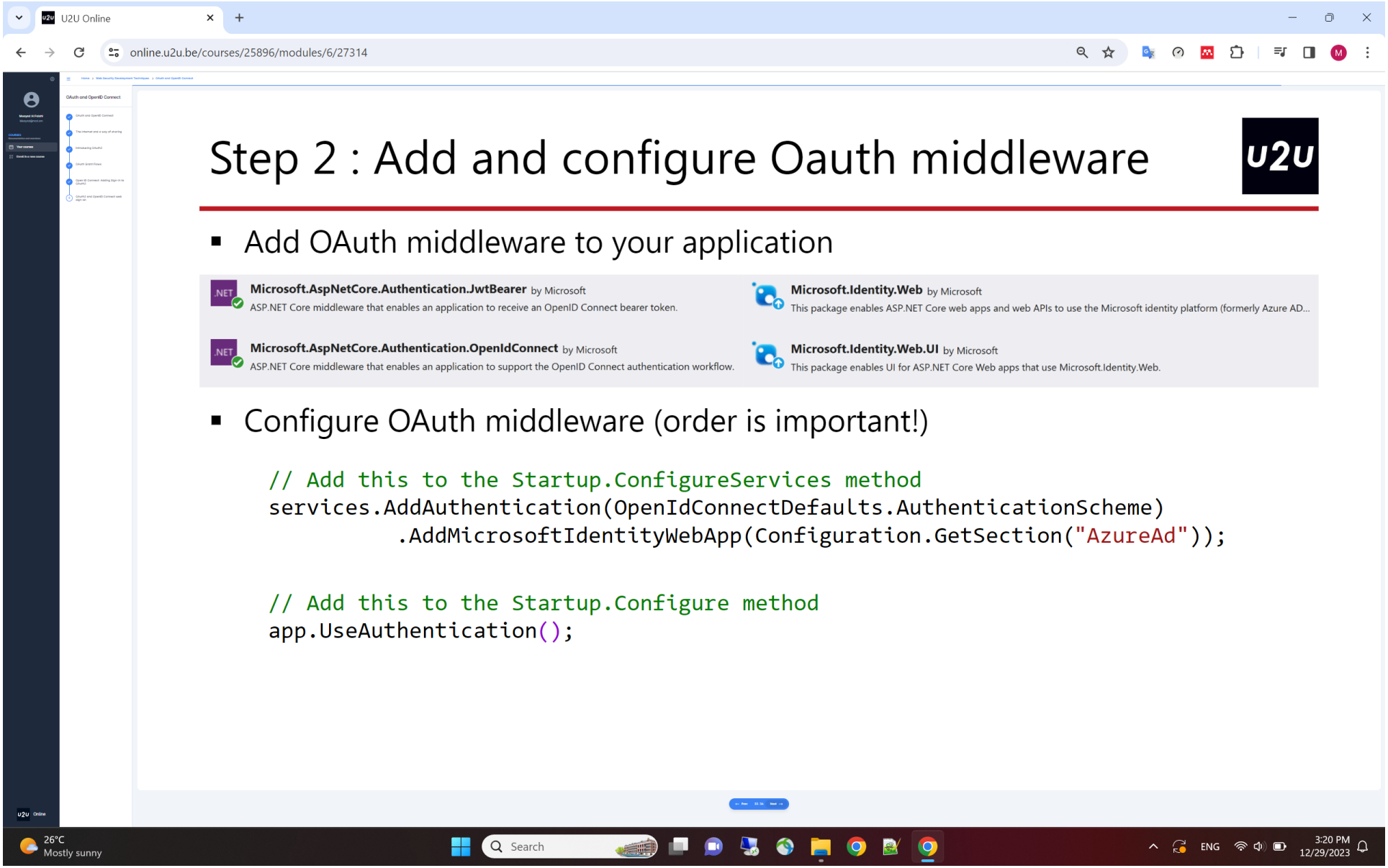

U2U Online
online.u2u.be/courses/25896/modules/6/27314
Implicit Grant Flow
U2U
SPA
B
Login +
Authorization
Authorization Server
26°C
Mostly sunny
Search
ENG
3:20 PM
12/29/2023

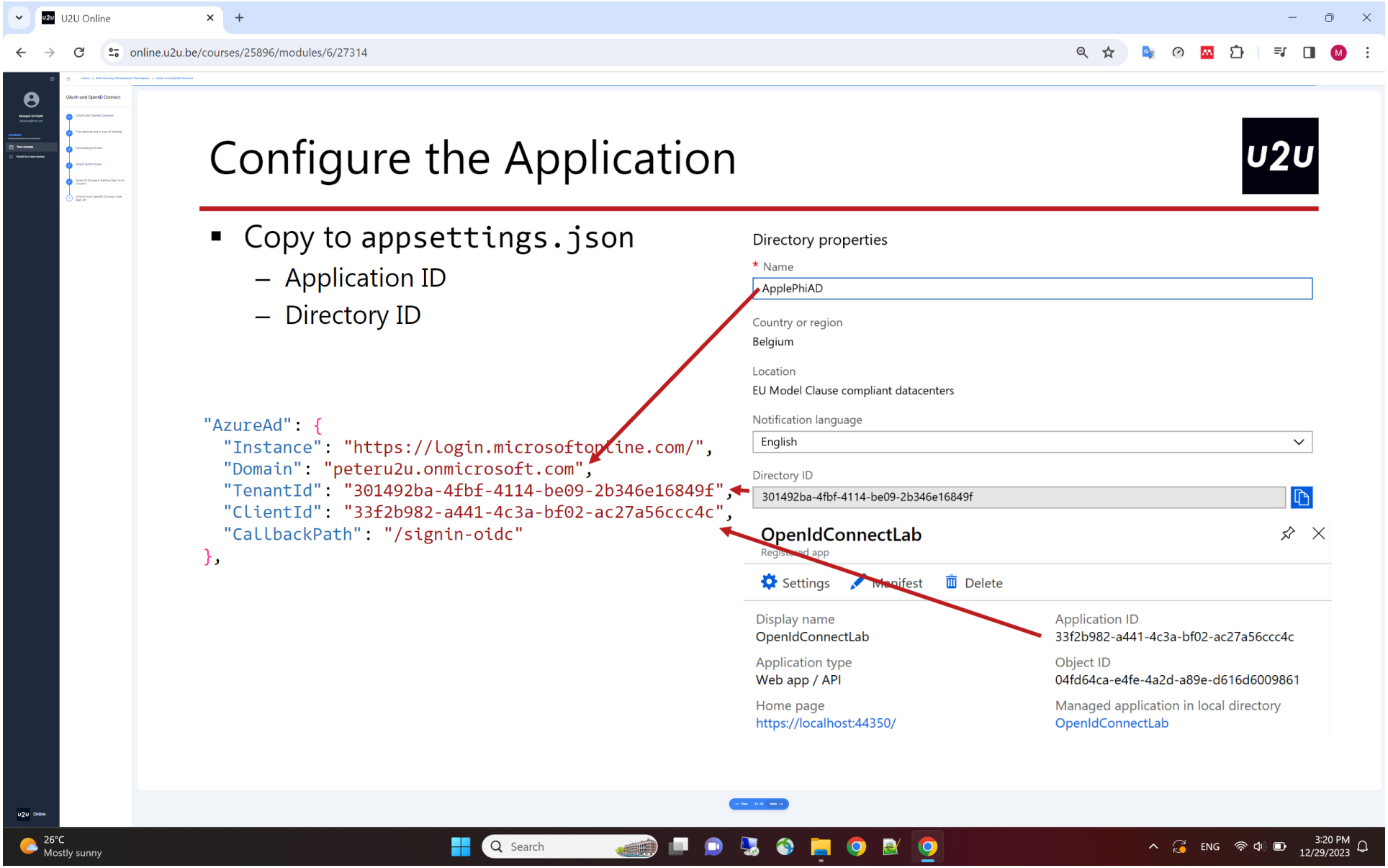

U2U Online
online.u2u.be/courses/25896/modules/6/27314
Hybrid Flow
u2u
A
B
1. Please do something
2. Redirect to AS
4. Code
Browser
3. Login + code +
Authorization
5. Code + Credentials
6.
7.
Token
Authorization Server
26°C
Mostly sunny
Search
ENG
3:20 PM
12/29/2023

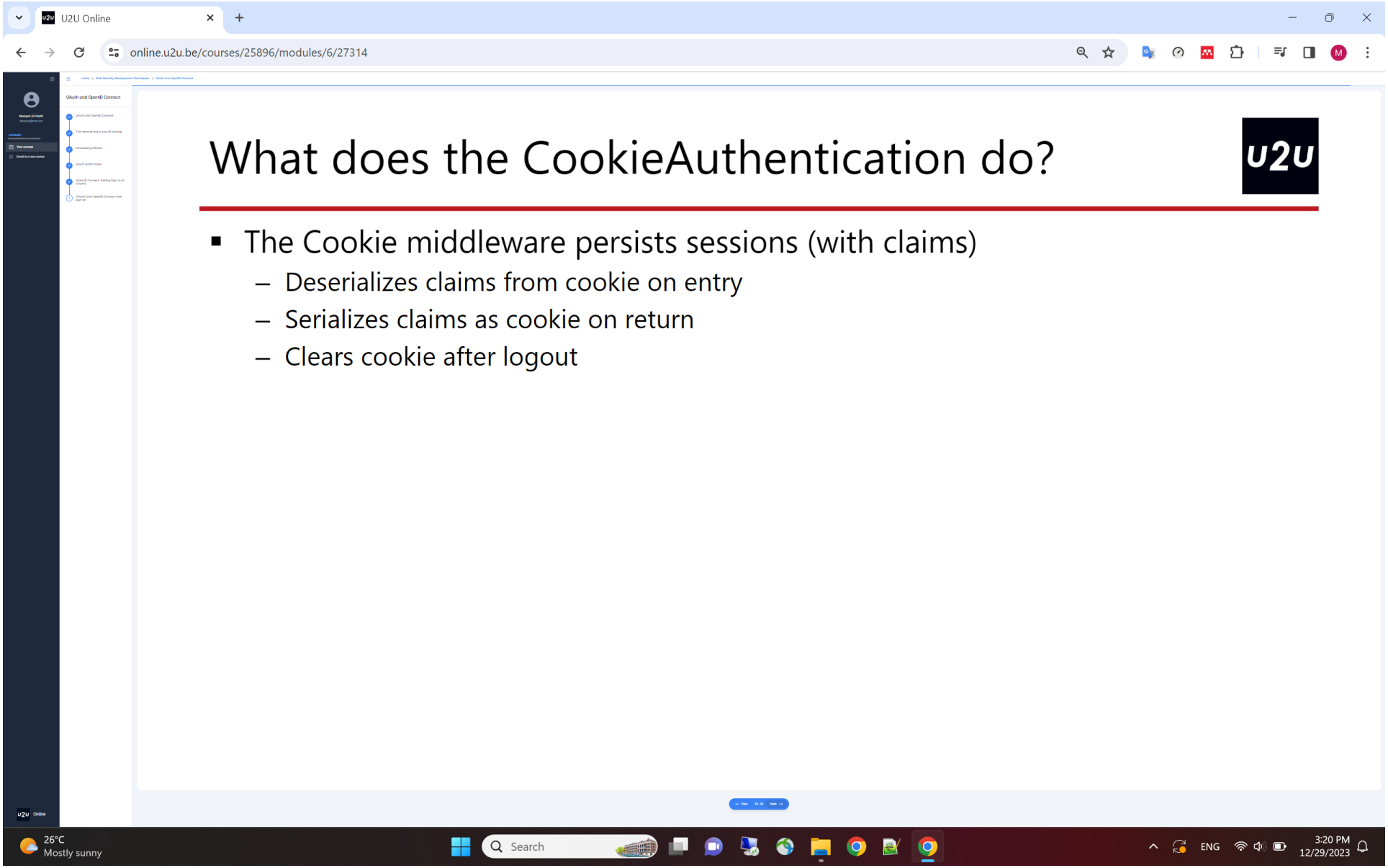

U2U Online
online.u2u.be/courses/25896/modules/6/27314
Using Microsoft Entra ID for web authentication
U2U
Step 1 : Register your application with Microsoft Entra ID
Step 2 : Add and configure OAuth2 middleware
26°C
Mostly sunny
Search
ENG
3:20 PM
12/29/2023

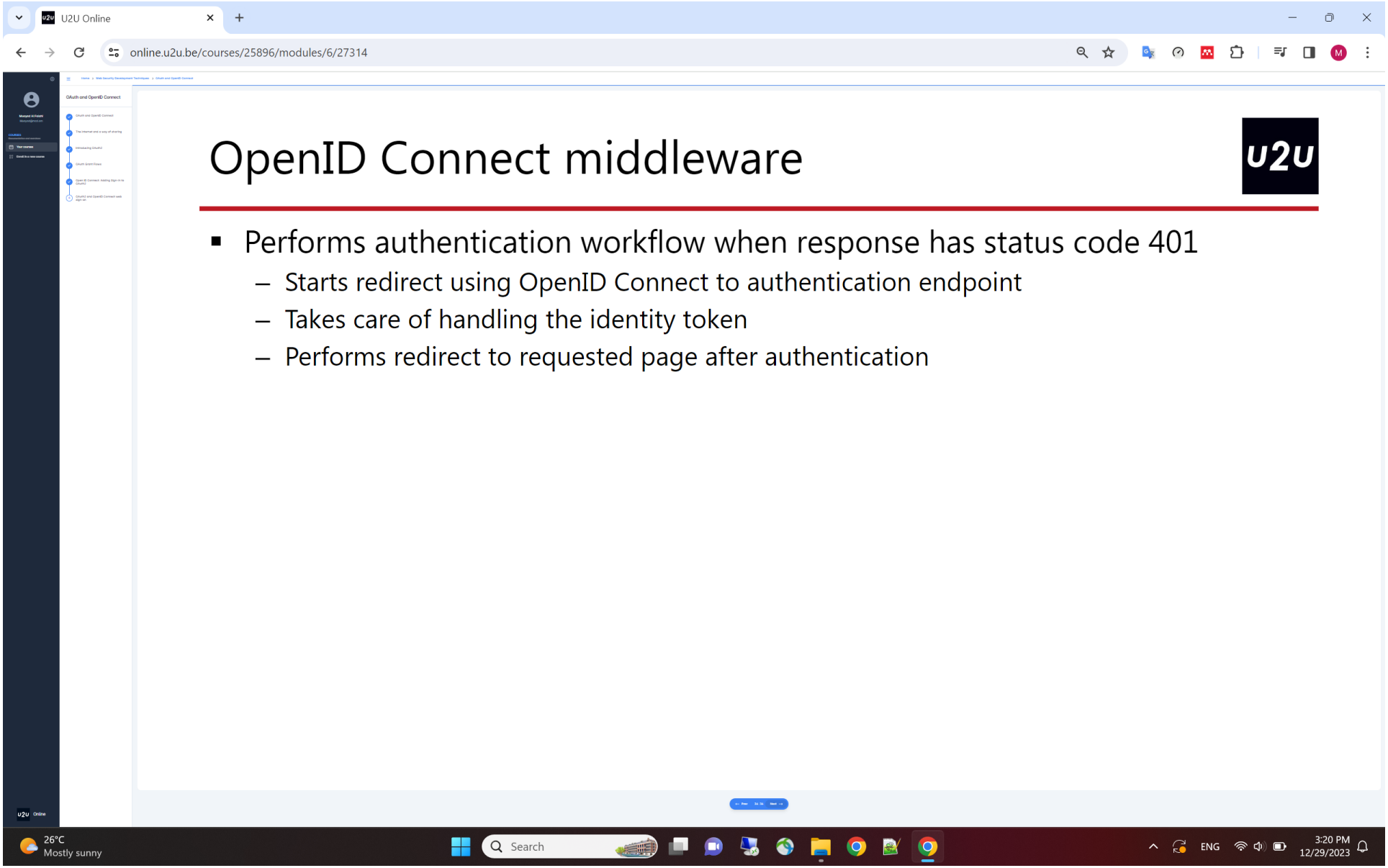

U2U Online
online.u2u.be/courses/25896/modules/6/27314
Step 1 : Register your application with Entra ID
U2U
Open Azure portal, and open Microsoft Entra ID
Microsoft Entra ID
Create a new application registration
App registrations
* Name
YourApp
Application type
Web app / API
* Sign-on URL
https://localhost:44350/signin-oidc
26°C
Mostly sunny
Search
ENG
3:20 PM
12/29/2023


U2U Online
online.u2u.be/courses/25896/modules/6/27314
OWIN Pipeline Processing Concept
u2u
Pipeline
Request
Middleware
Middleware
Middleware
Middleware
Reponse
26°C
Mostly sunny
Search
ENG
3:20 PM
12/29/2023


U2U Online
online.u2u.be/courses/25896/modules/6/27314
Step 2 : Add and configure Oauth middleware
U2U
Add OAuth middleware to your application
Microsoft.AspNetCore.Authentication.JwtBearer by Microsoft
ASP.NET Core middleware that enables an application to receive an OpenID Connect bearer token.
Microsoft.Identity.Web by Microsoft
This package enables ASP.NET Core web apps and web APIs to use the Microsoft identity platform (formerly Azure AD...
Microsoft.AspNetCore.Authentication.OpenIdConnect by Microsoft
ASP.NET Core middleware that enables an application to support the OpenID Connect authentication workflow.
Microsoft.Identity.Web.UI by Microsoft
This package enables UI for ASP.NET Core Web apps that use Microsoft.Identity.Web.
Configure OAuth middleware (order is important!)
// Add this to the Startup.ConfigureServices method
services.AddAuthentication(OpenIdConnectDefaults.AuthenticationScheme)
.AddMicrosoftIdentityWebApp(Configuration.GetSection("AzureAd"));
// Add this to the Startup.Configure method
app.UseAuthentication();
26°C
Mostly sunny
Search
ENG
3:20 PM
12/29/2023


U2U Online
online.u2u.be/courses/25896/modules/6/27314
Configure the Application
u2u
Copy to appsettings.json
Application ID
Directory ID
"AzureAd": {
"Instance": "https://login.microsoftonline.com/",
"Domain": "peteru2u.onmicrosoft.com",
"TenantId": "301492ba-4fbf-4114-be09-2b346e16849f",
"ClientId": "33f2b982-a441-4c3a-bf02-ac27a56ccc4c",
"CallbackPath": "/signin-oidc"
},
Directory properties
* Name
ApplePhiAD
Country or region
Belgium
Location
EU Model Clause compliant datacenters
Notification language
English
Directory ID
301492ba-4fbf-4114-be09-2b346e16849f
OpenIdConnectLab
Registered app
Settings
Manifest
Delete
Display name
OpenIdConnectLab
Application ID
33f2b982-a441-4c3a-bf02-ac27a56ccc4c
Application type
Web app / API
Object ID
04fd64ca-e4fe-4a2d-a89e-d616d6009861
Home page
https://localhost:44350/
Managed application in local directory
OpenIdConnectLab
26°C
Mostly sunny
Search
ENG
3:20 PM
12/29/2023


U2U Online
online.u2u.be/courses/25896/modules/6/27314
What does the CookieAuthentication do?
u2u
The Cookie middleware persists sessions (with claims)
Deserializes claims from cookie on entry
Serializes claims as cookie on return
Clears cookie after logout
26°C
Mostly sunny
Search
ENG
3:20 PM
12/29/2023


U2U Online
online.u2u.be/courses/25896/modules/6/27314
OpenID Connect middleware
u2u
Performs authentication workflow when response has status code 401
Starts redirect using OpenID Connect to authentication endpoint
Takes care of handling the identity token
Performs redirect to requested page after authentication
26°C
Mostly sunny
Search
ENG
3:20 PM
12/29/2023