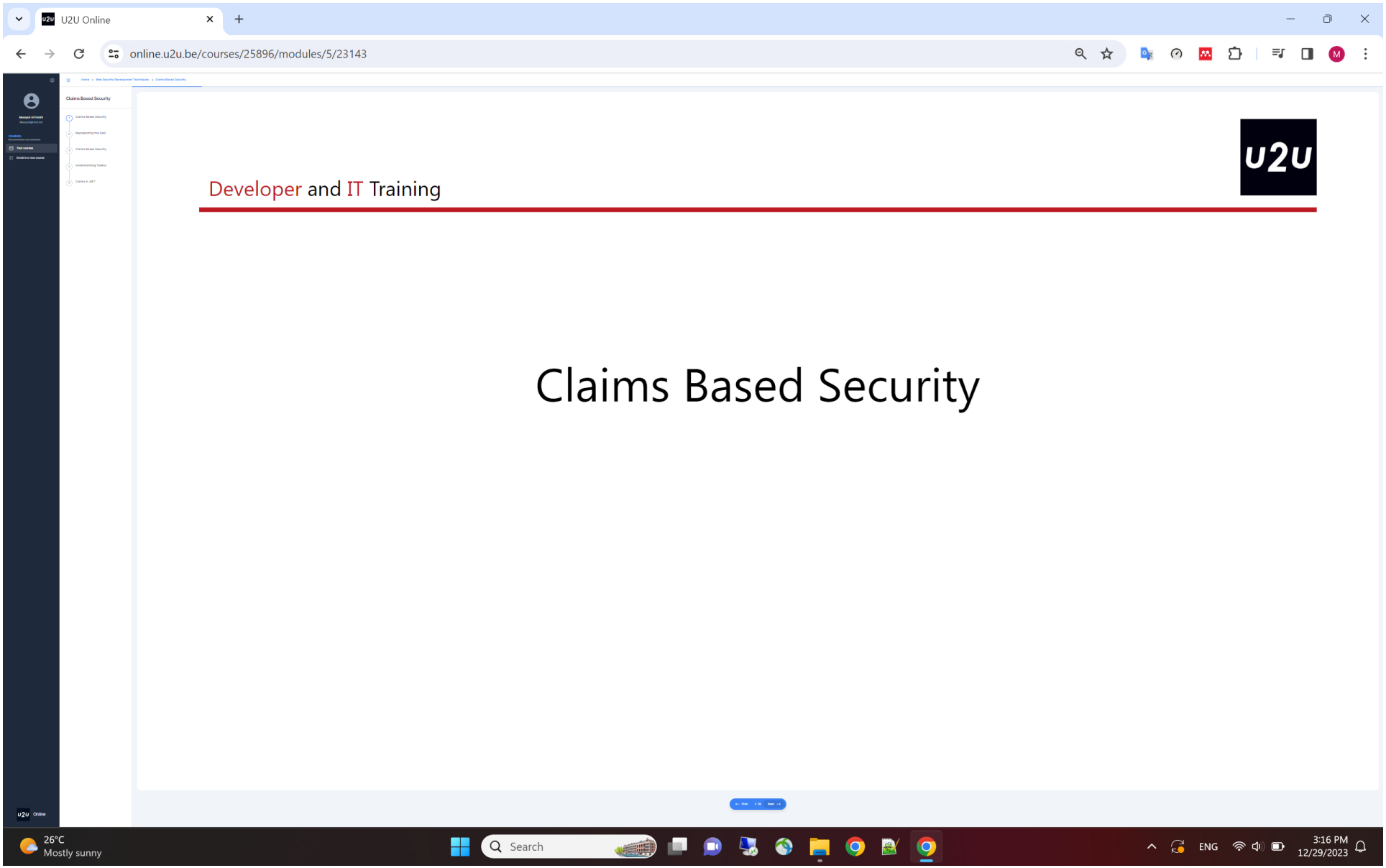
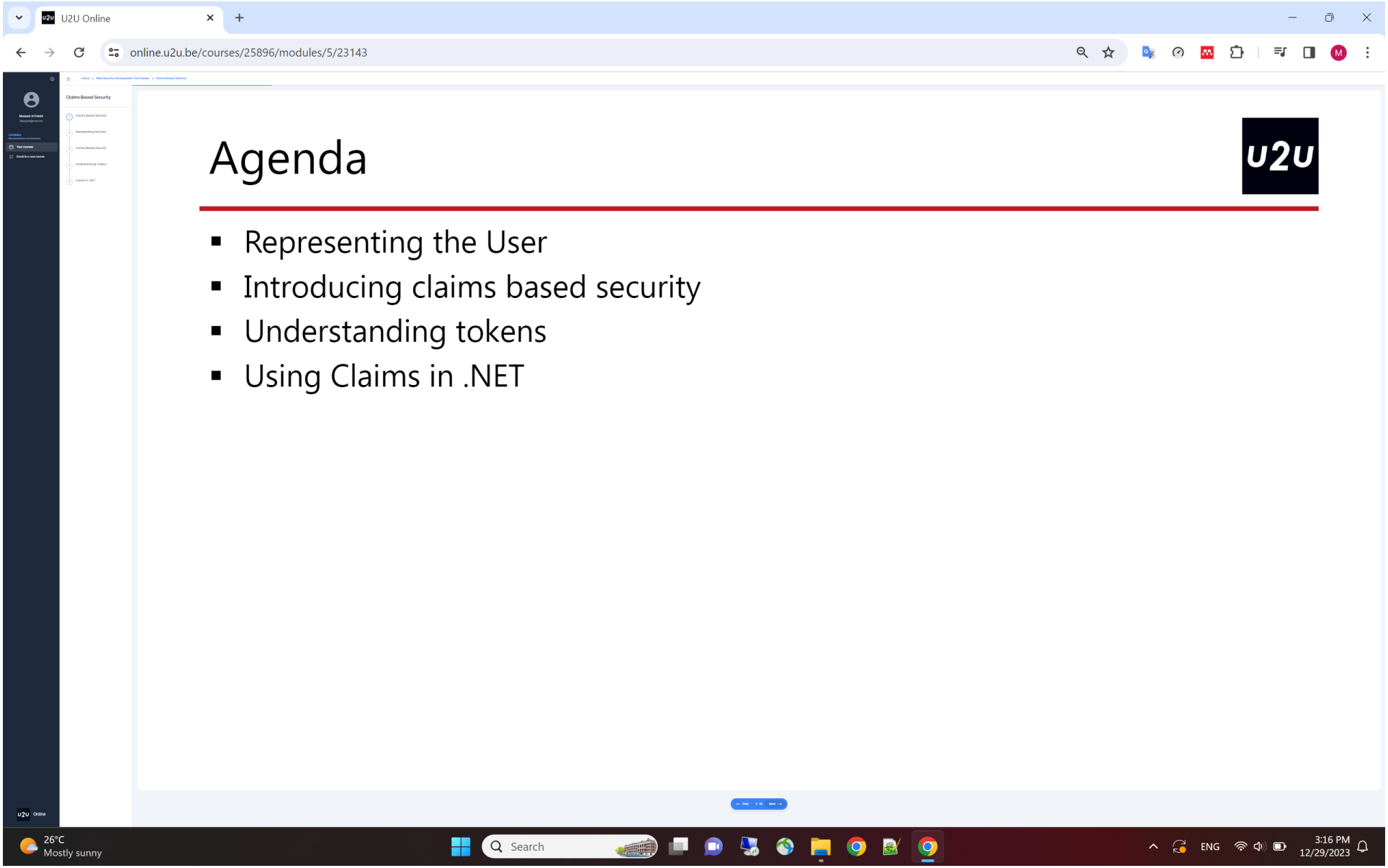
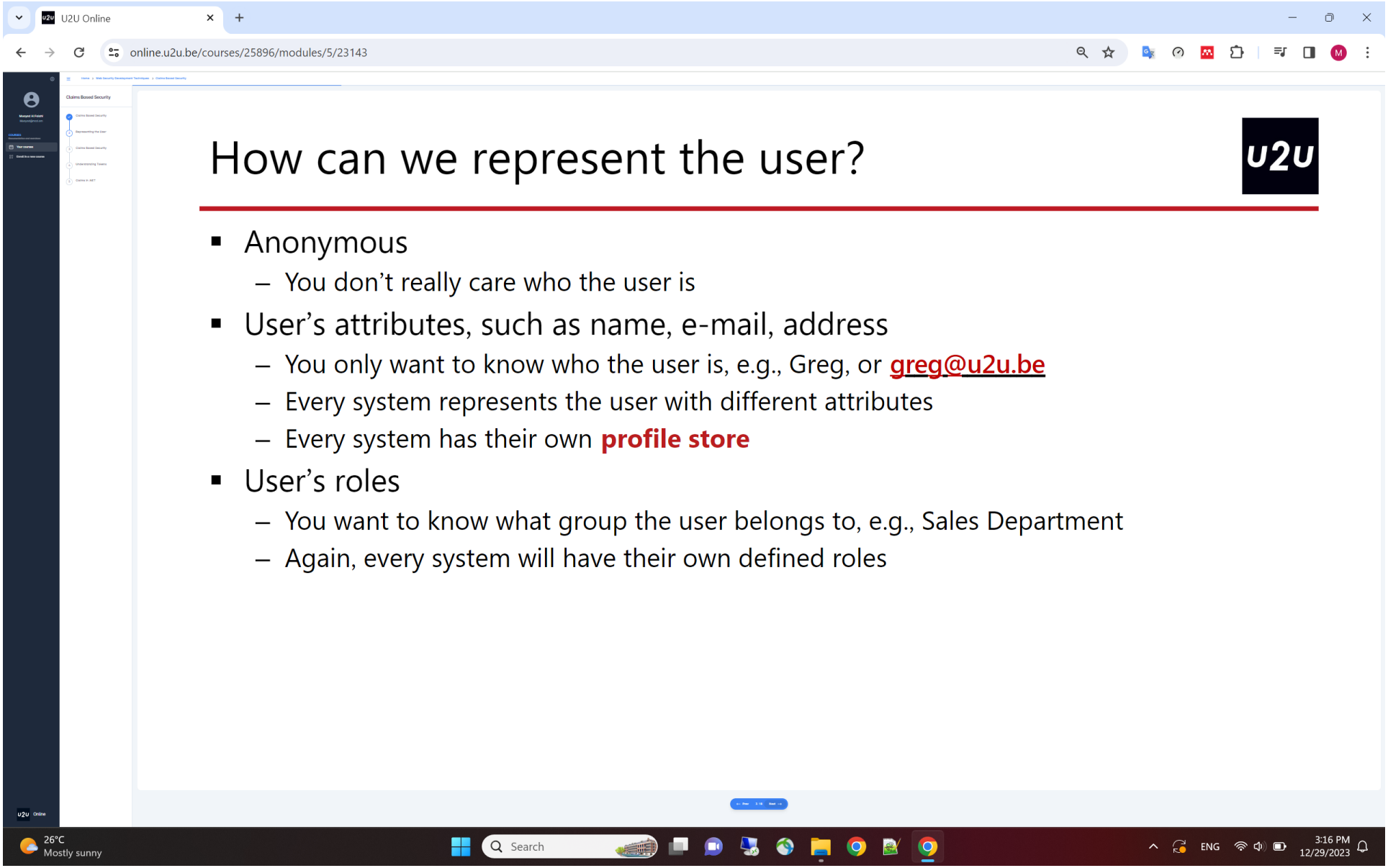
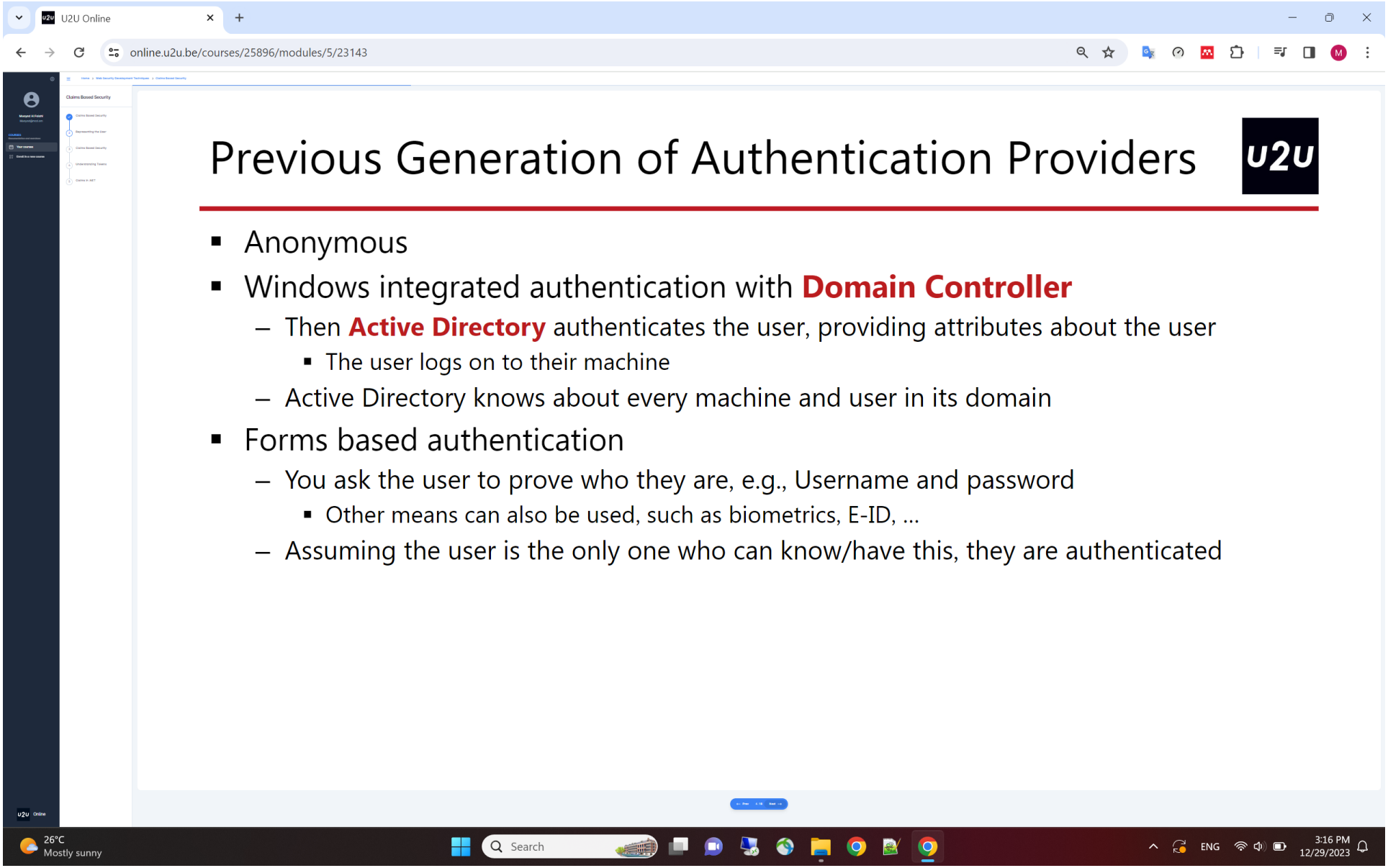
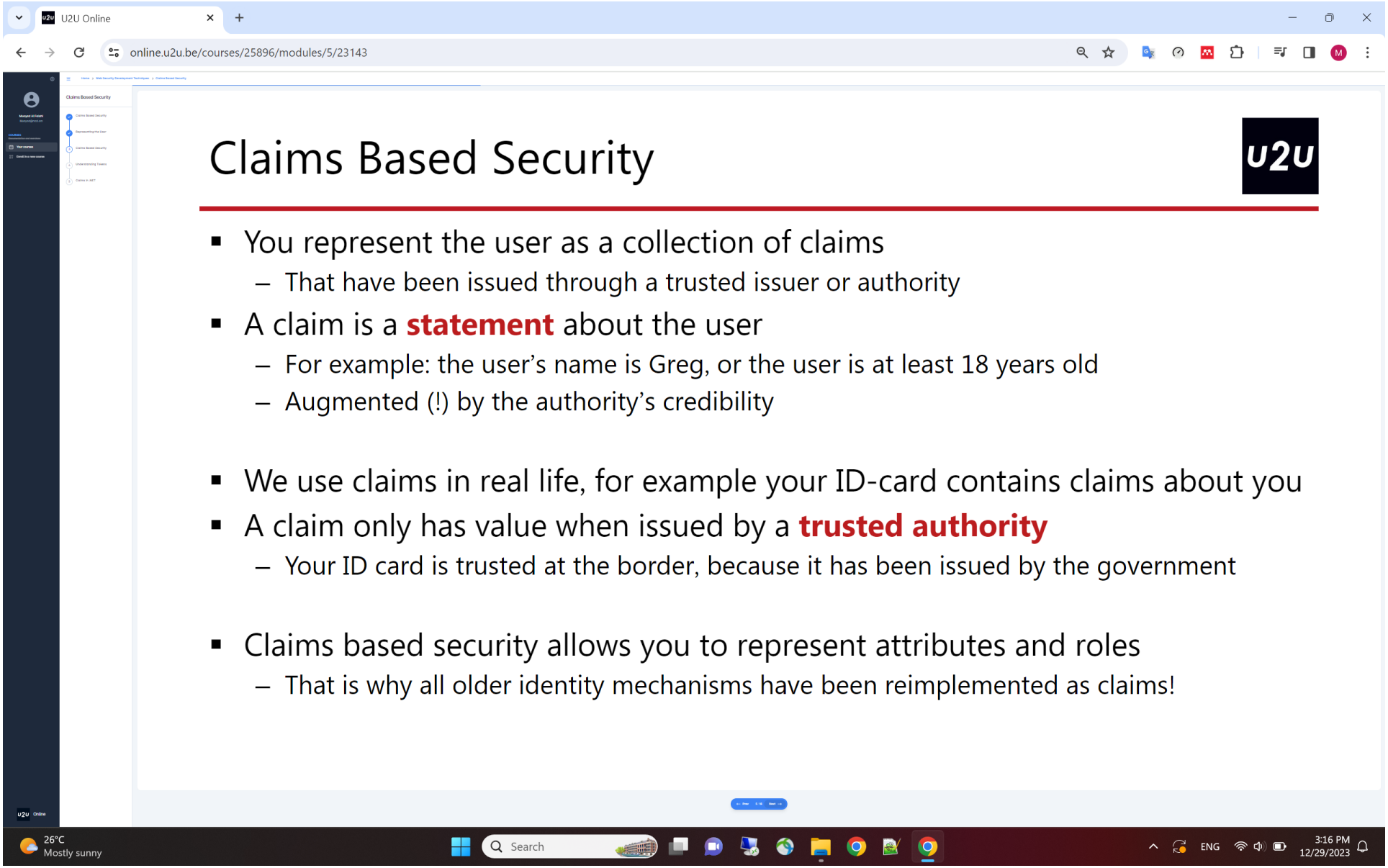
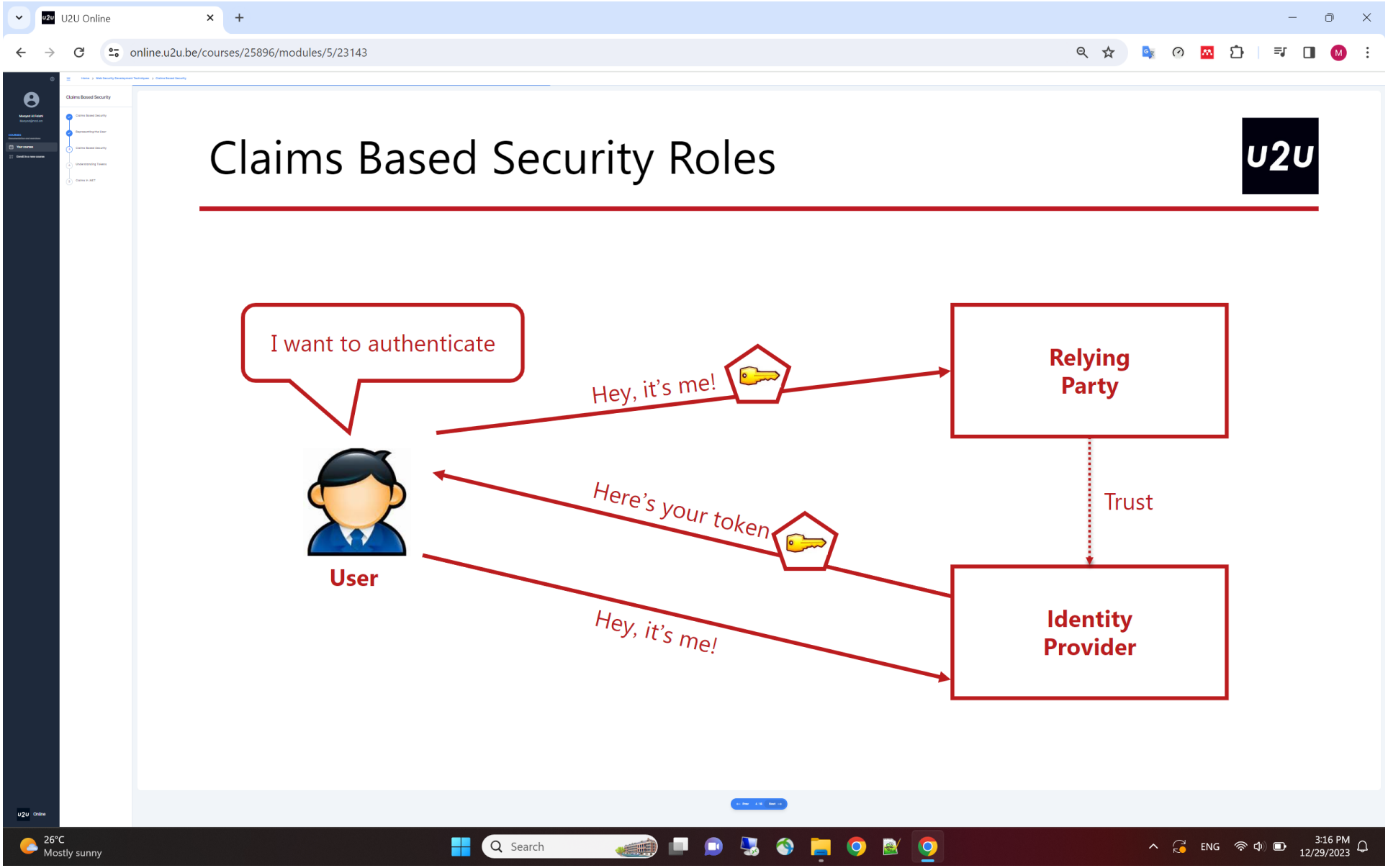

U2U Online
online.u2u.be/courses/25896/modules/5/23143
Developer and IT Training
U2U
Claims Based Security
26°C
Mostly sunny
Search
ENG
3:16 PM
12/29/2023

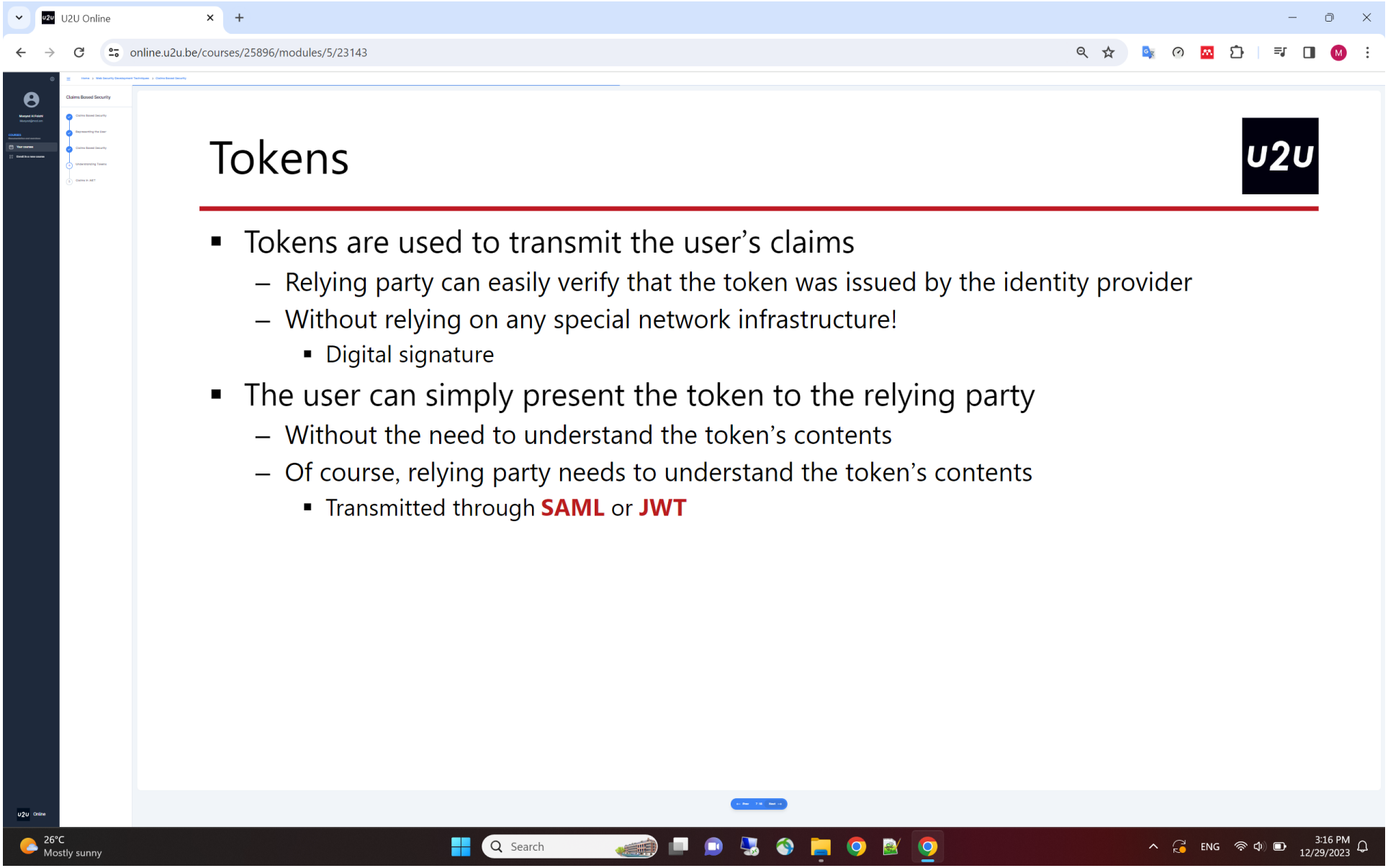

U2U Online
online.u2u.be/courses/25896/modules/5/23143
Claims Based Security
Agenda
U2U
Representing the User
Introducing claims based security
Understanding tokens
Using Claims in .NET
26°C
Mostly sunny
Search
ENG
3:16 PM
12/29/2023


U2U Online
online.u2u.be/courses/25896/modules/5/23143
How can we represent the user?
U2U
Anonymous
You don't really care who the user is
User's attributes, such as name, e-mail, address
You only want to know who the user is, e.g., Greg, or greg@u2u.be
Every system represents the user with different attributes
Every system has their own profile store
User's roles
You want to know what group the user belongs to, e.g., Sales Department
Again, every system will have their own defined roles
26°C
Mostly sunny
Search
ENG
3:16 PM
12/29/2023


U2U Online
online.u2u.be/courses/25896/modules/5/23143
Previous Generation of Authentication Providers
U2U
Anonymous
Windows integrated authentication with Domain Controller
Then Active Directory authenticates the user, providing attributes about the user
The user logs on to their machine
Active Directory knows about every machine and user in its domain
Forms based authentication
You ask the user to prove who they are, e.g., Username and password
Other means can also be used, such as biometrics, E-ID, ...
Assuming the user is the only one who can know/have this, they are authenticated
26°C
Mostly sunny
Search
ENG
3:16 PM
12/29/2023


U2U Online
online.u2u.be/courses/25896/modules/5/23143
Claims Based Security
U2U
Claims Based Security
You represent the user as a collection of claims
That have been issued through a trusted issuer or authority
A claim is a statement about the user
For example: the user's name is Greg, or the user is at least 18 years old
Augmented (!) by the authority's credibility
We use claims in real life, for example your ID-card contains claims about you
A claim only has value when issued by a trusted authority
Your ID card is trusted at the border, because it has been issued by the government
Claims based security allows you to represent attributes and roles
That is why all older identity mechanisms have been reimplemented as claims!
26°C
Mostly sunny
Search
ENG
3:16 PM
12/29/2023

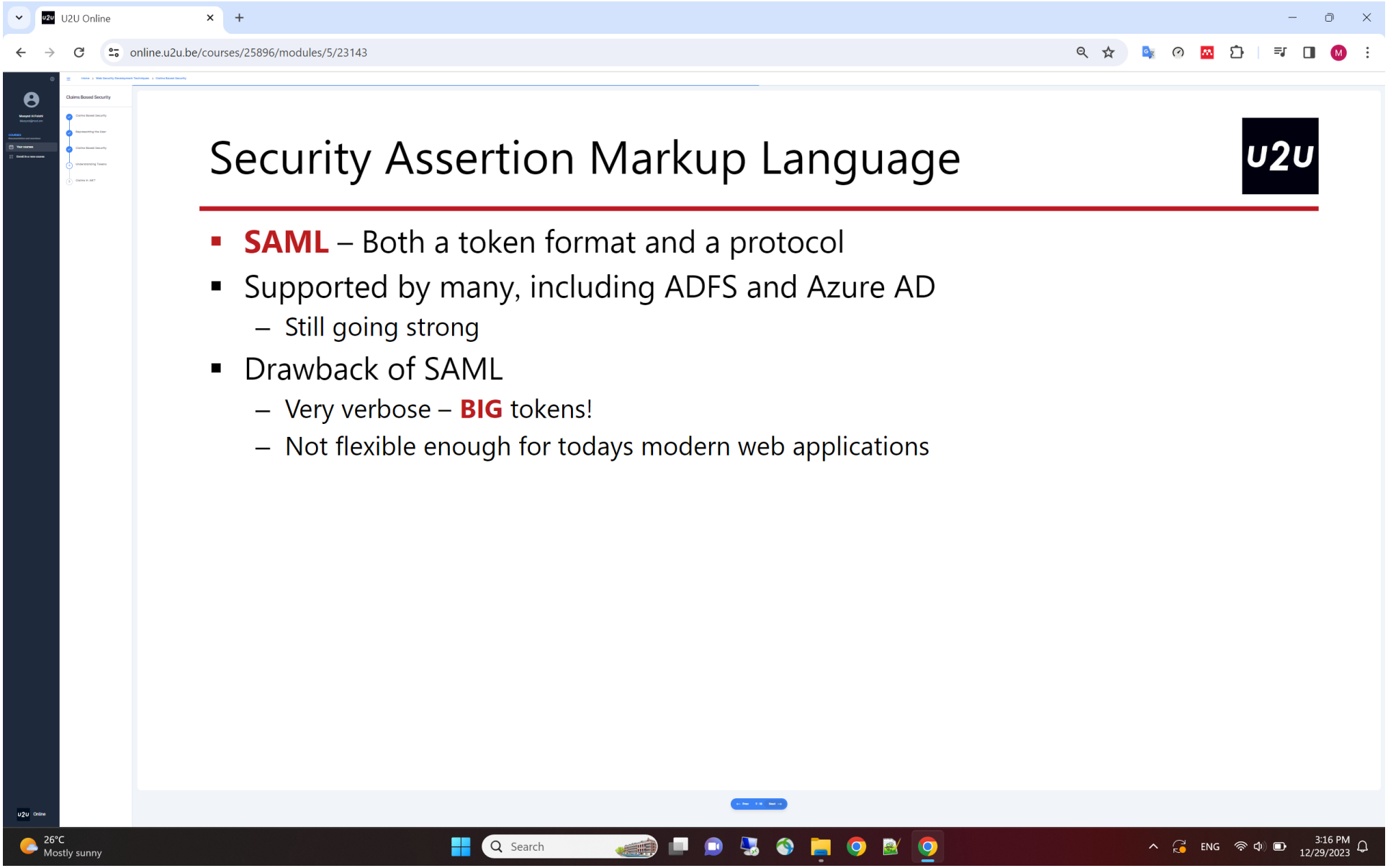

U2U Online
online.u2u.be/courses/25896/modules/5/23143
Claims Based Security Roles
U2U
I want to authenticate
Hey, it's me!
Relying Party
Trust
Here's your token
User
Hey, it's me!
Identity Provider
26°C
Mostly sunny
Search
ENG
3:16 PM
12/29/2023

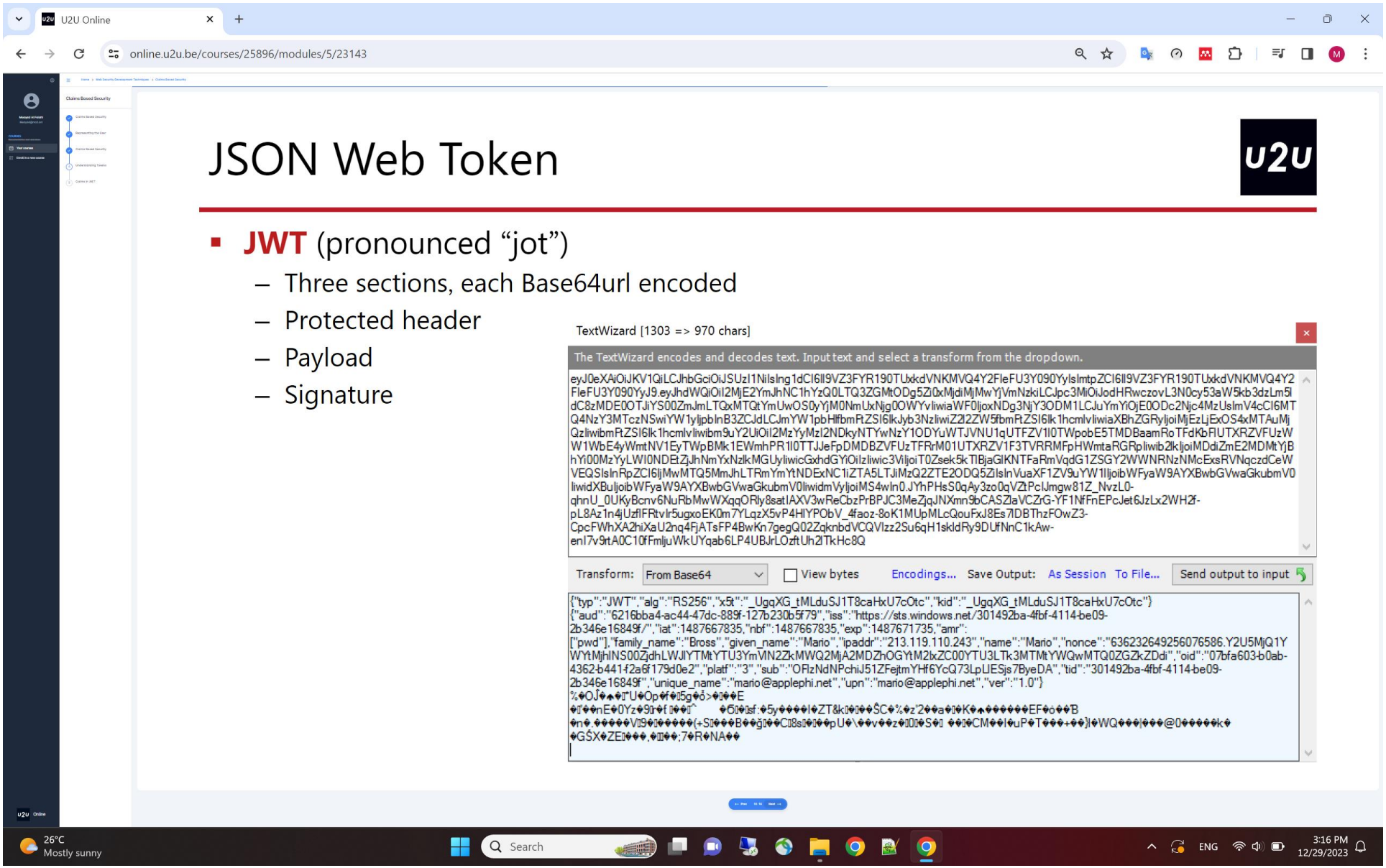

U2U Online
online.u2u.be/courses/25896/modules/5/23143
Claims Based Security
Tokens
u2u
Tokens are used to transmit the user's claims
Relying party can easily verify that the token was issued by the identity provider
Without relying on any special network infrastructure!
Digital signature
The user can simply present the token to the relying party
Without the need to understand the token's contents
Of course, relying party needs to understand the token's contents
Transmitted through SAML or JWT
26°C
Mostly sunny
Search
ENG
3:16 PM
12/29/2023

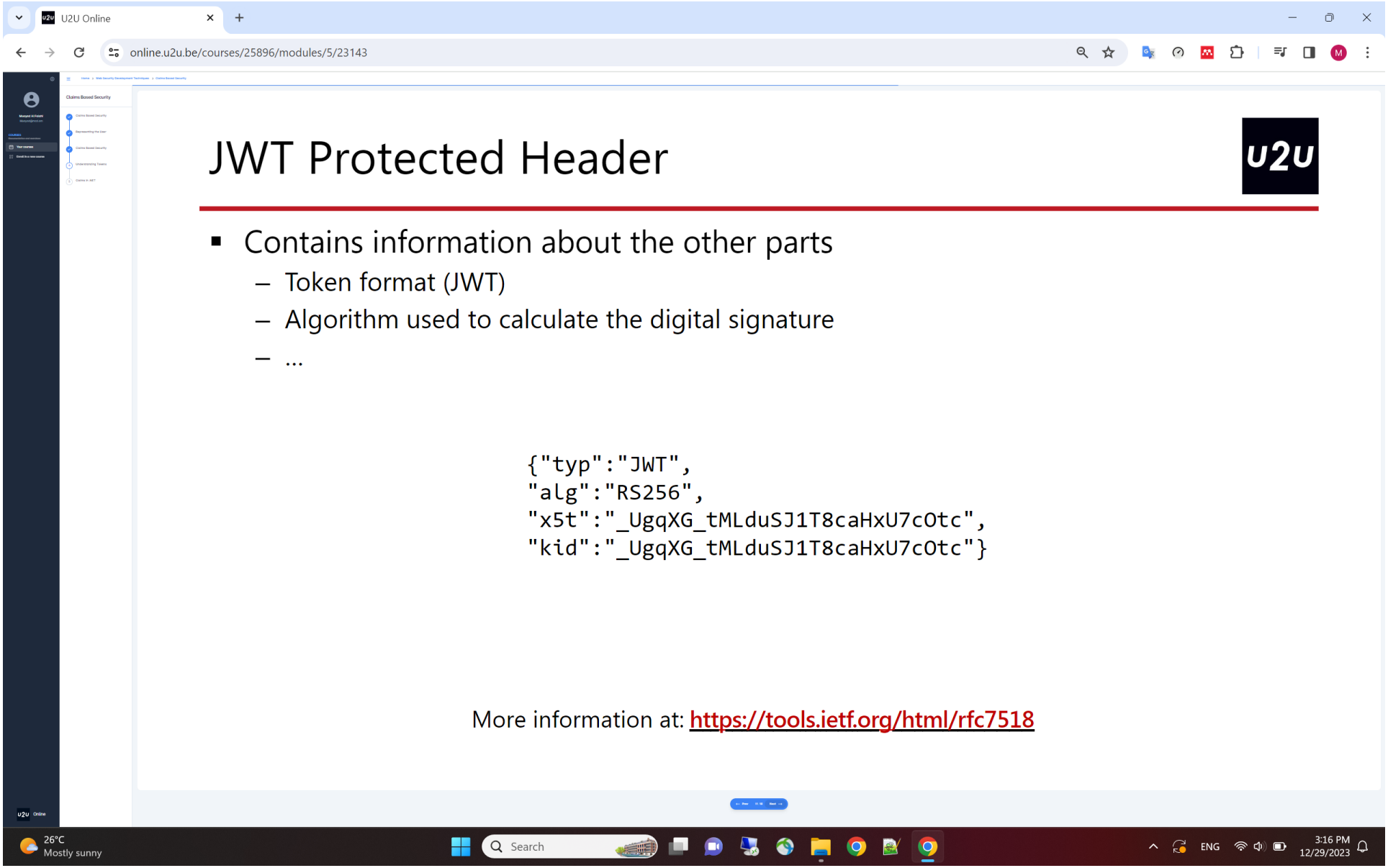
U2U Online

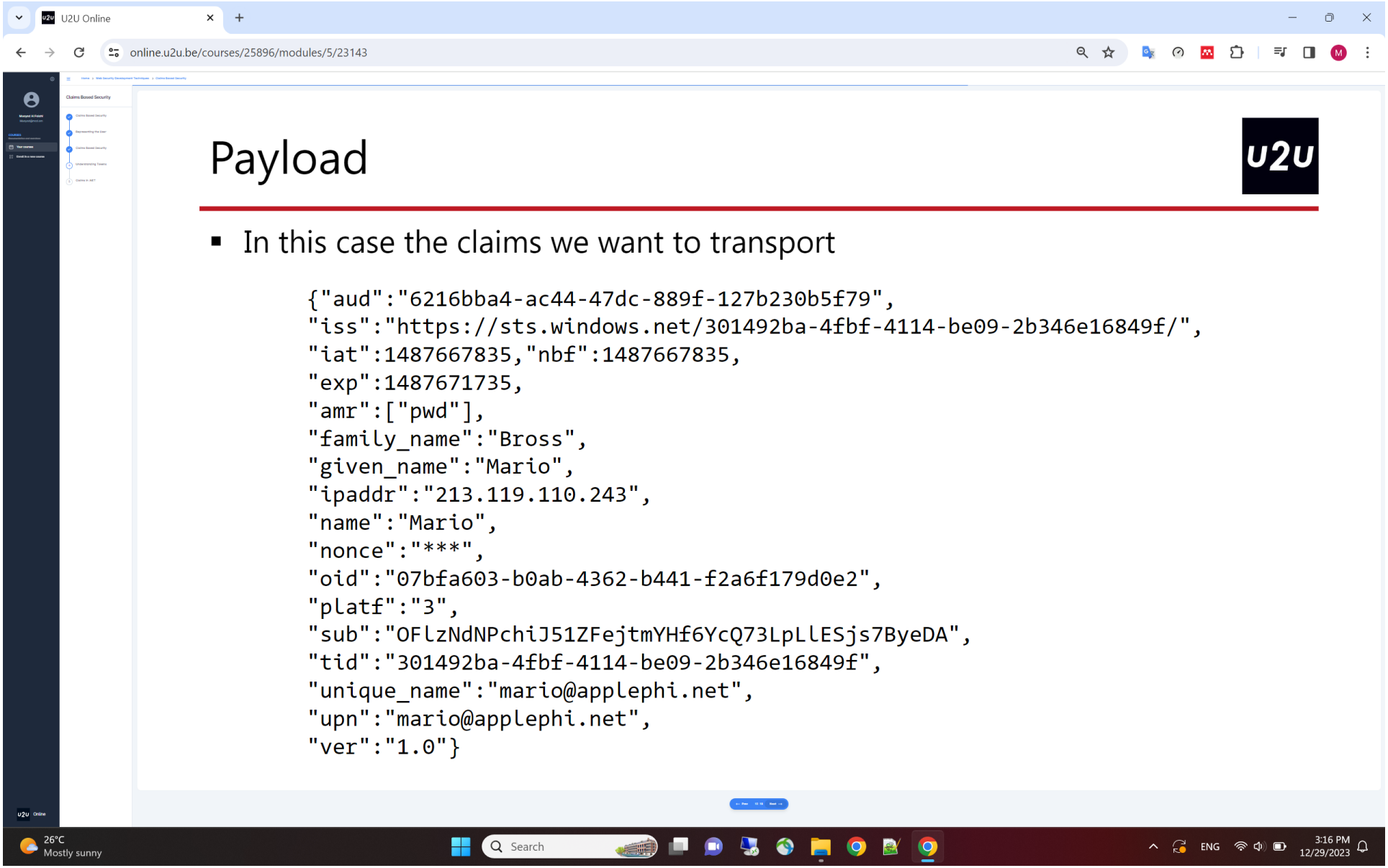
online.u2u.be/courses/25896/modules/5/23143

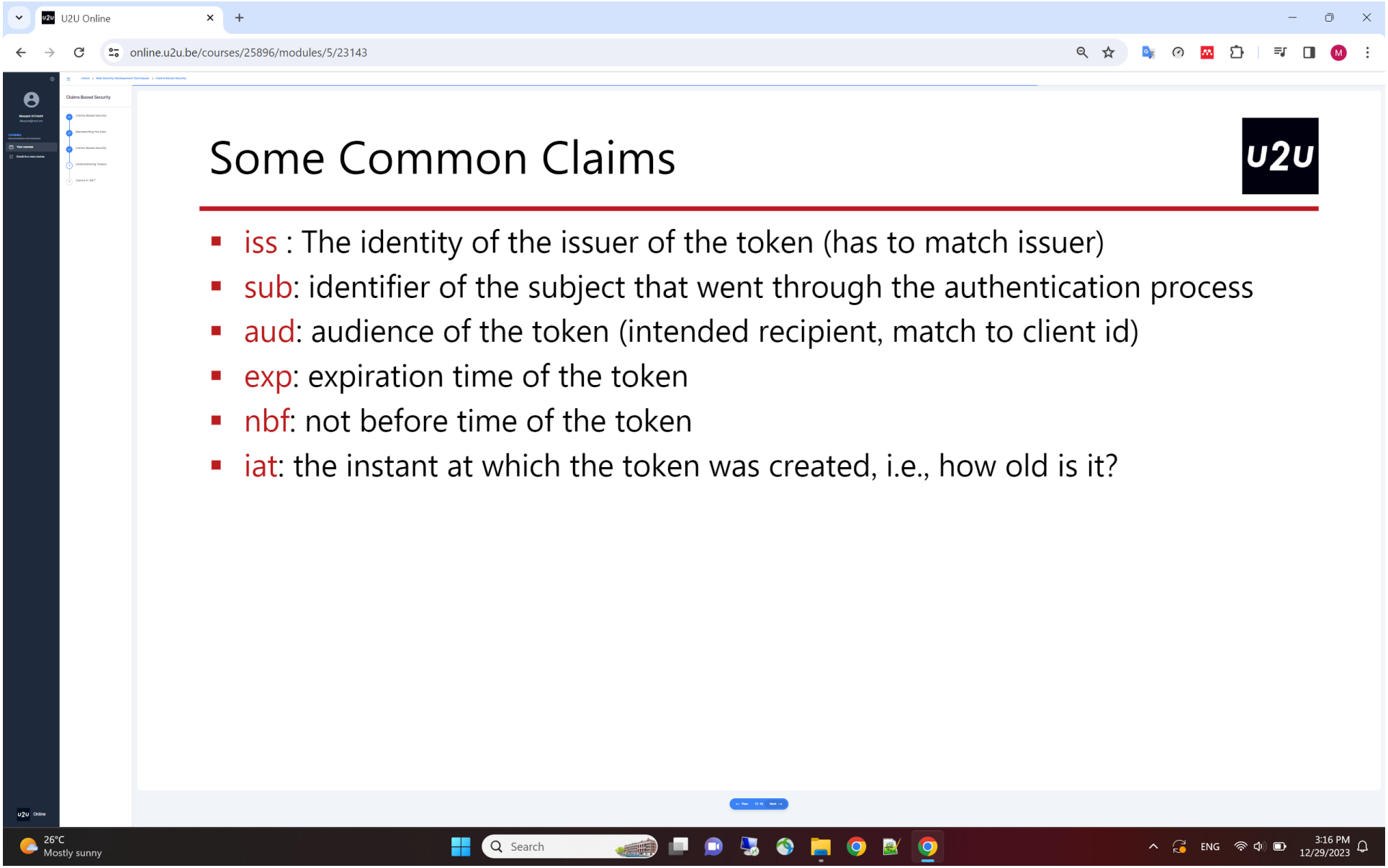
Token Example

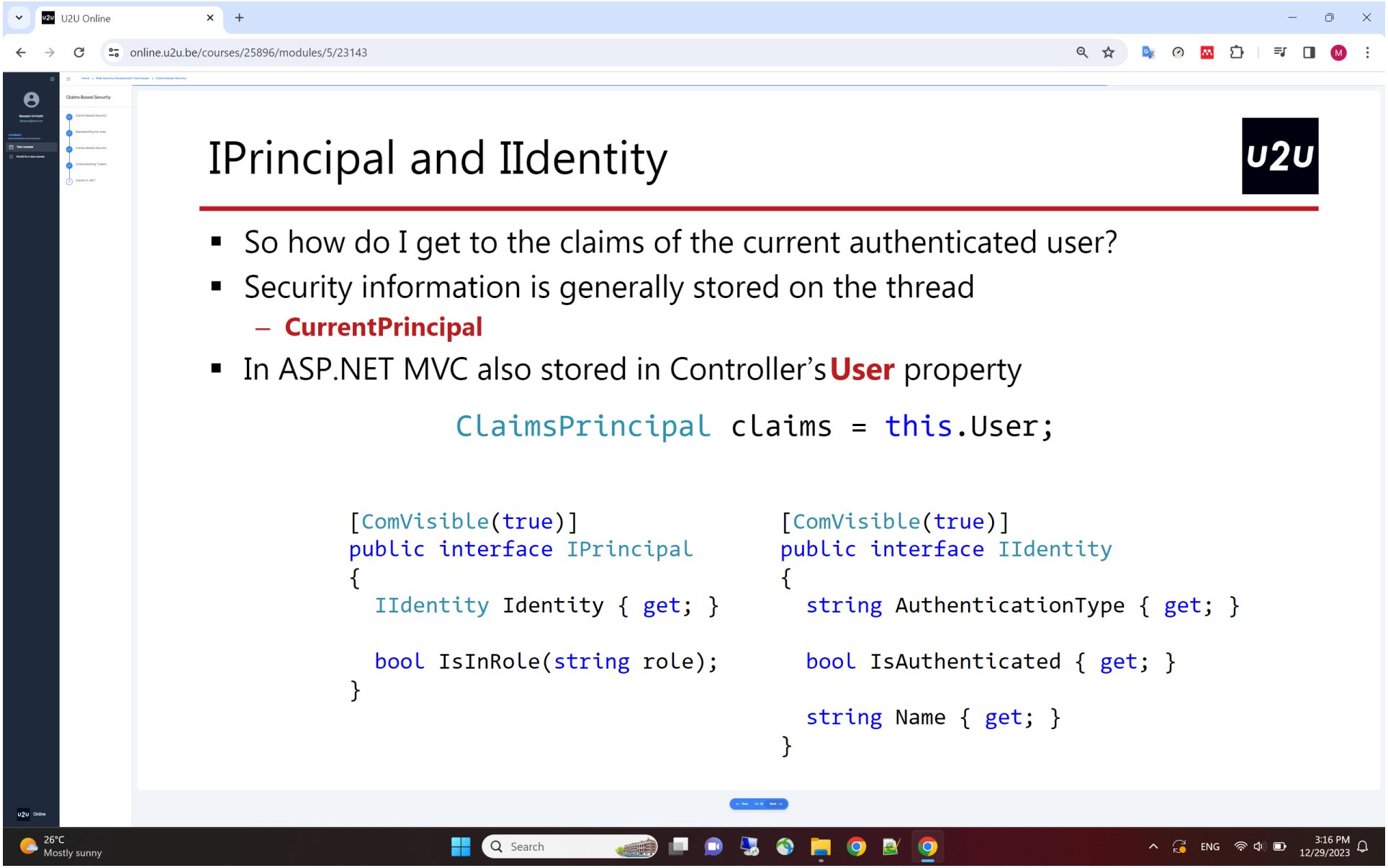

U2U Online
online.u2u.be/courses/25896/modules/5/23143
Claims Based Security
Security Assertion Markup Language
U2U
SAML – Both a token format and a protocol
Supported by many, including ADFS and Azure AD
Still going strong
Drawback of SAML
Very verbose – BIG tokens!
Not flexible enough for todays modern web applications
26°C
Mostly sunny
Search
ENG
3:16 PM
12/29/2023

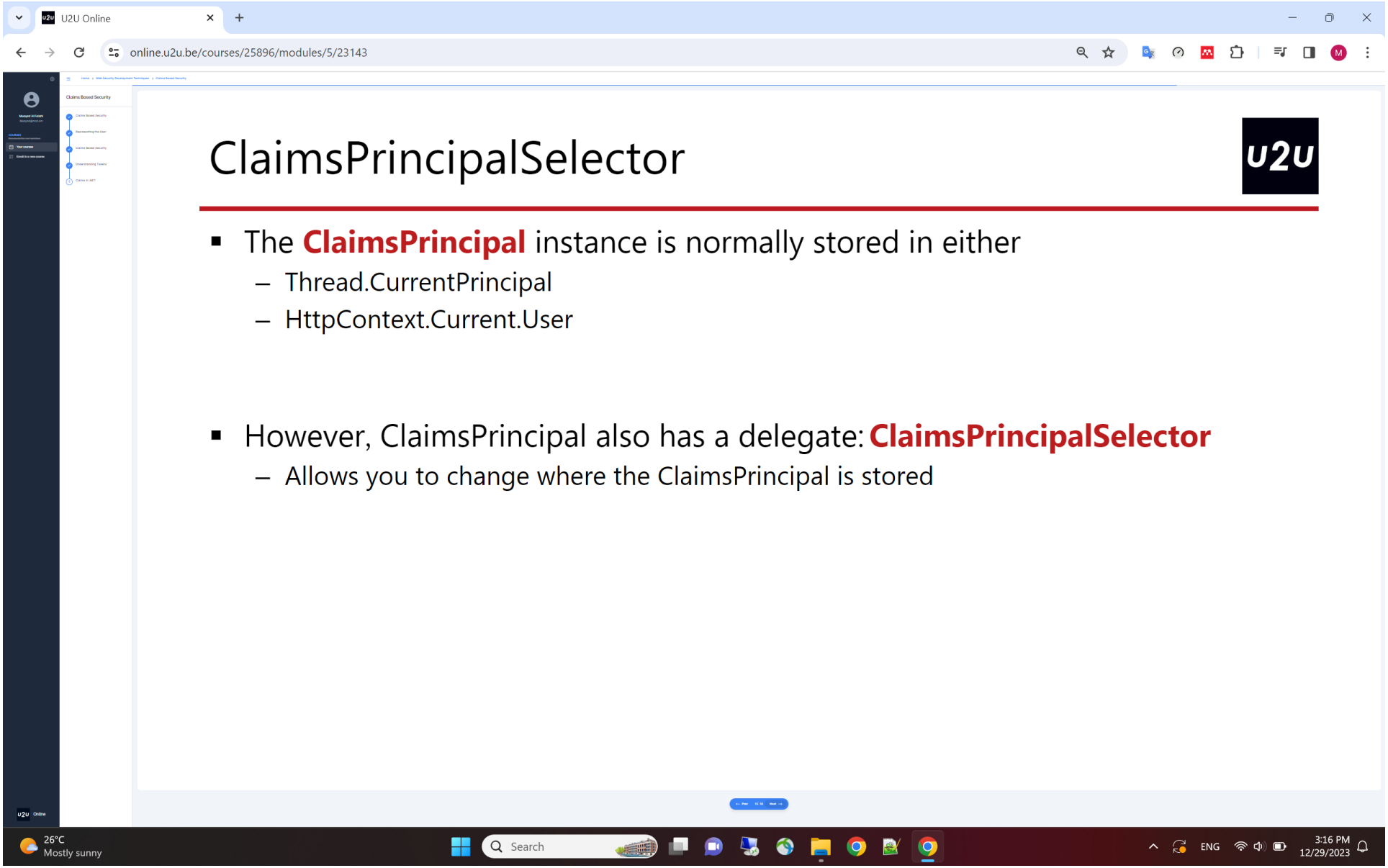

U2U Online
online.u2u.be/courses/25896/modules/5/23143
JSON Web Token
u2u
JWT (pronounced “jot”)
Three sections, each Base64url encoded
Protected header
Payload
Signature
TextWizard [1303 => 970 chars]
The TextWizard encodes and decodes text. Input text and select a transform from the dropdown.
eyJ0eXAiOiJKV1QiLCJhbGciOiJSUzI1NiIsIng1dCI6Il9VZ3FYR190TUxkdVNKMVQ4Y2FleFU3Y090YyIsImtpZCI6Il9VZ3FYR190TUxkdVNKMVQ4Y2
FleFU3Y090YyJ9.eyJhdWQiOiI2MjE2YmJhNC1hYzQ0LTQ3ZGMtODg5Zi0xMjdiMjMwYjVmNzkiLCJpc3MiOiJodHRwczovL3N0cy53aW5kb3dzLm5l
dC8zMDE0OTJiYS00ZmJmLTQxMTQtYmUwOS0yYjM0NmUxNjg0OWYvIiwiaWF0IjoxNDg3NjY3ODM1LCJuYmYiOjE0ODc2Njc4MzUsImV4cCI6MT
Q4NzY3MTczNSwiYW1yIjpbInB3ZCJdLCJmYW1pbHlfbmFtZSI6Ik1hcmlvIiwiaXBhZGRyIjoiMjEzLjExOS4xMTAuMj
QzIiwibmFtZSI6Ik1hcmlvIiwibm9uY2UiOiI2MzYyMzI2NDkyNTYwNzY1ODYuWTJVNU1qUTFZV1I0TWpobE5TMDBaamRoTFdKbFlUTXRZVFUzW
W1WbE4yWmtNV1EyTWpBMk1EWmhPR1I0TTJJeFpDMDBZVFUzTFRrM01UTXRZV1F3TVRRMFpHWmtaRGRpliwib2lkIjoiMDdiZmE2MDMtYjB
hYi00MzYyLWI0NDEtZjJhNmYxNzlkMGUyliwicGxhdGYiOiIzIiwic3ViIjoiT0Zsek5kTlBjaGlKNTFaRmVqdG1ZSGY2WWNRNzNMcExsRVNqczdCeW
VEQSIsInRpZCI6IjMwMTQ5MmJhLTRmYmYtNDExNC1iZTA5LTJiMzQ2ZTE2ODQ5ZiIsInVuaXF1ZV9uYW1lIjoibWFyaW9AYXBwbGVwaGkubmV0
liwidXBuIjoibWFyaW9AYXBwbGVwaGkubmV0liwidmVyIjoiMS4wIn0.JYhPHsS0qAy3zo0qVZtPclJmgw81Z_NvzL0-
qhnU_0UKyBcnv6NuRbMwWXqqORly8satIAXV3wReCbzPrBPJC3MeZjqJNXmn9bCASZlaVCZrG-YF1NfFnEPcJet6JzLx2WH2f-
pL8Az1n4jUzfIFRtvIr5ugxoEK0m7YLqzX5vP4HIYPObV_4faoz-8oK1MUpMLcQouFxJ8Es7lDBThzFOwZ3-
CpcFWhXA2hiXaU2nq4FjATsFP4BwKn7gegQ02ZqknbdVCQVlzz2Su6qH1skldRy9DUfNnC1kAw-
enI7v9rtA0C10fFmljuWkUYqab6LP4UBJrLOzftUh2lTkHc8Q
Transform:
From Base64
View bytes
Encodings...
Save Output:
As Session
To File...
Send output to input
{"typ":"JWT","alg":"RS256","x5t":"_UgqXG_tMLduSJ1T8caHxU7cOtc","kid":"_UgqXG_tMLduSJ1T8caHxU7cOtc"}
{"aud":"6216bba4-ac44-47dc-889f-127b230b5f79","iss":"https://sts.windows.net/301492ba-4fbf-4114-be09-
2b346e16849f/","iat":1487667835,"nbf":1487667835,"exp":1487671735,"amr":
["pwd"],"family_name":"Bross","given_name":"Mario","ipaddr":"213.119.110.243","name":"Mario","nonce":"636232649256076586.Y2U5MjQ1Y
WYtMjhlNS00ZjdhLWJlYTMtYTU3YmVlN2ZkMWQ2MjA2MDZhOGYtM2IxZC00YTU3LTk3MTMtYWQwMTQ0ZGZkZDdi","oid":"07bfa603-b0ab-
4362-b441-f2a6f179d0e2","platf":"3","sub":"OFlzNdNPchiJ51ZFejtmYHf6YcQ73LpLIESjs7ByeDA","tid":"301492ba-4fbf-4114-be09-
2b346e16849f","unique_name":"mario@applephi.net","upn":"mario@applephi.net","ver":"1.0"}
%♦OJ♦♠♦▯"U♦Op♦f♦▯5g♦ó>♦▯♦♦E
♦▯♦♦nE♦0Yz♦9▯r♦f▯♦♦▯^ ♦5▯♦▯sf:♦5y♦♦♦♦l♦ZT&k▯♦▯♦♦ŠC♦%♦z'2♦♦a♦▯♦K♦♠♦♦♦♦♦♦EF♦ó♦♦B
♦n♦.♦♦♦♦♦V▯9♦▯♦♦♦♦♦(+S▯♦♦♦B♦♦g▯♦♦C▯8s▯♦▯♦♦pU♦\♦♦v♦♦z♦▯▯♦S♦▯ ♦♦▯♦CM♦♦l♦uP♦T♦♦♦+♦♦}l♦WQ♦♦♦|♦♦♦@0♦♦♦♦♦k♦
♦GŚX♦ZE▯♦♦♦,♦▯♦♦;7♦R♦NA♦♦
26°C
Mostly sunny
Search
ENG
3:16 PM
12/29/2023

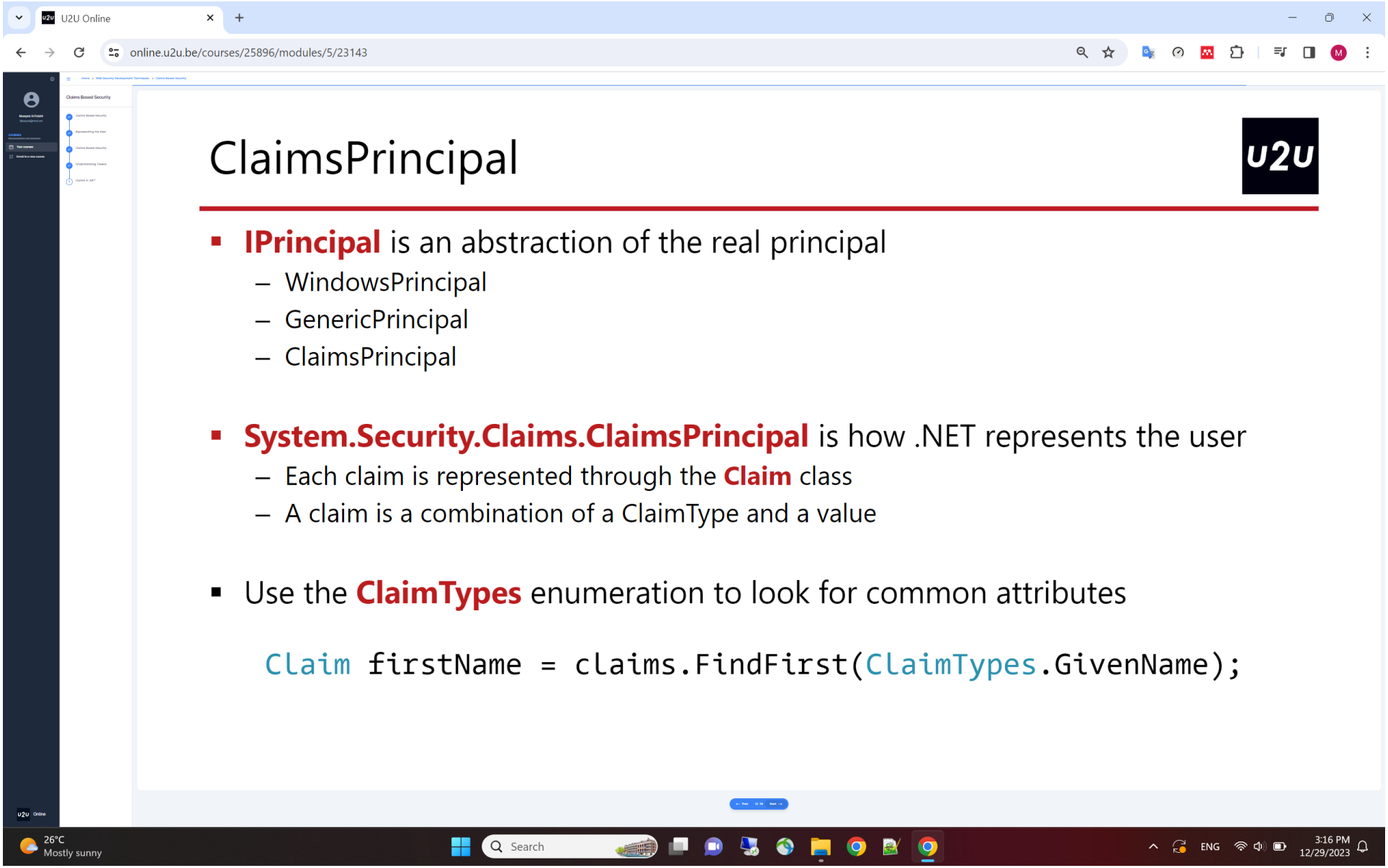

U2U Online
online.u2u.be/courses/25896/modules/5/23143
JWT Protected Header
u2u
Contains information about the other parts
Token format (JWT)
Algorithm used to calculate the digital signature
...
{"typ":"JWT",
"alg":"RS256",
"x5t":"_UgqXG_tMLduSJ1T8caHxU7cOtc",
"kid":"_UgqXG_tMLduSJ1T8caHxU7cOtc"}
More information at: https://tools.ietf.org/html/rfc7518
26°C
Mostly sunny
Search
ENG
3:16 PM
12/29/2023

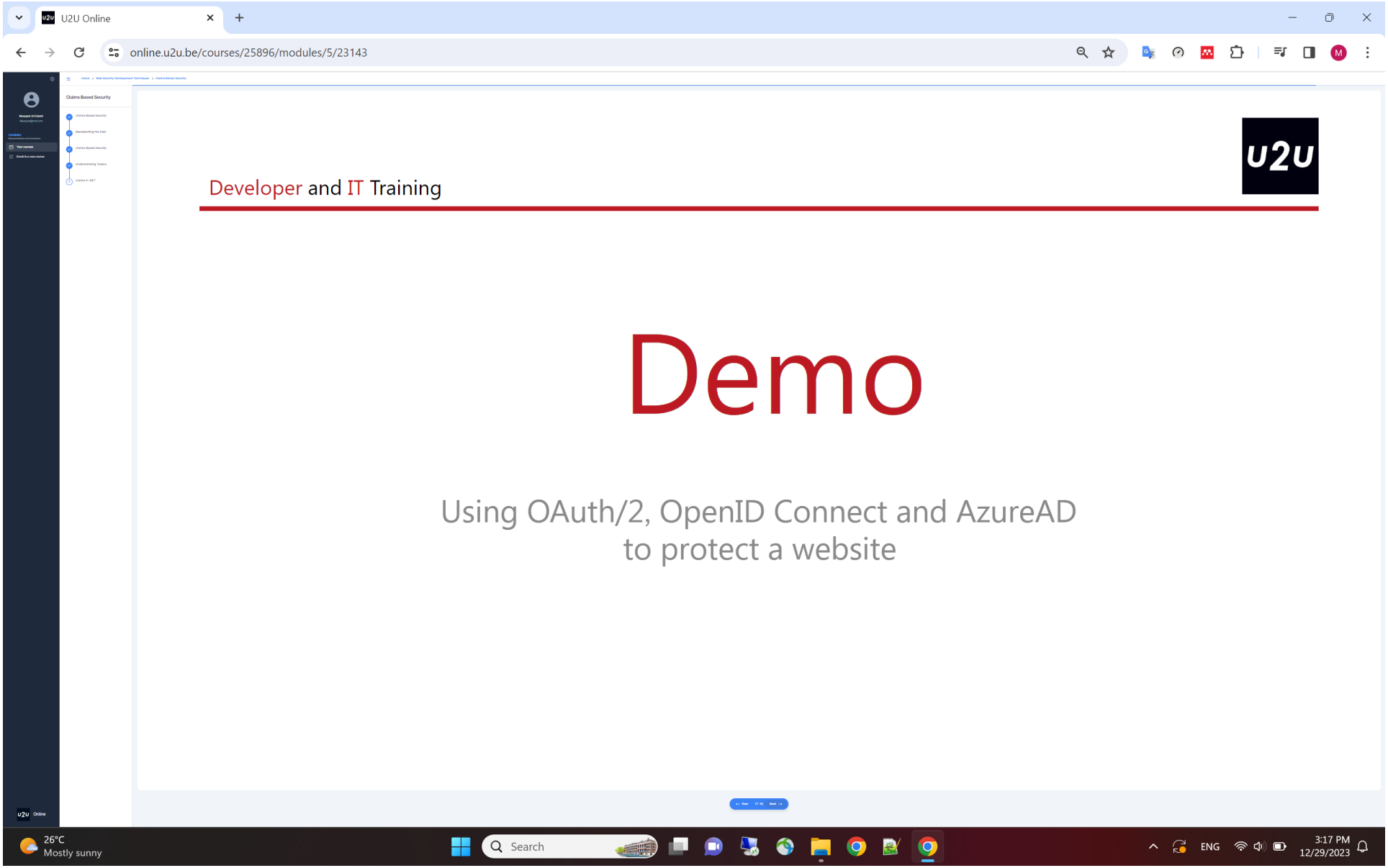

U2U Online
online.u2u.be/courses/25896/modules/5/23143
Payload
U2U
In this case the claims we want to transport
{"aud":"6216bba4-ac44-47dc-889f-127b230b5f79",
"iss":"https://sts.windows.net/301492ba-4fbf-4114-be09-2b346e16849f/",
"iat":1487667835,"nbf":1487667835,
"exp":1487671735,
"amr":["pwd"],
"family_name":"Bross",
"given_name":"Mario",
"ipaddr":"213.119.110.243",
"name":"Mario",
"nonce":"***",
"oid":"07bfa603-b0ab-4362-b441-f2a6f179d0e2",
"platf":"3",
"sub":"OFlzNdNPchiJ51ZFejtmYHf6YcQ73LpLlESjs7ByeDA",
"tid":"301492ba-4fbf-4114-be09-2b346e16849f",
"unique_name":"mario@applephi.net",
"upn":"mario@applephi.net",
"ver":"1.0"}
26°C
Mostly sunny
Search
ENG
3:16 PM
12/29/2023

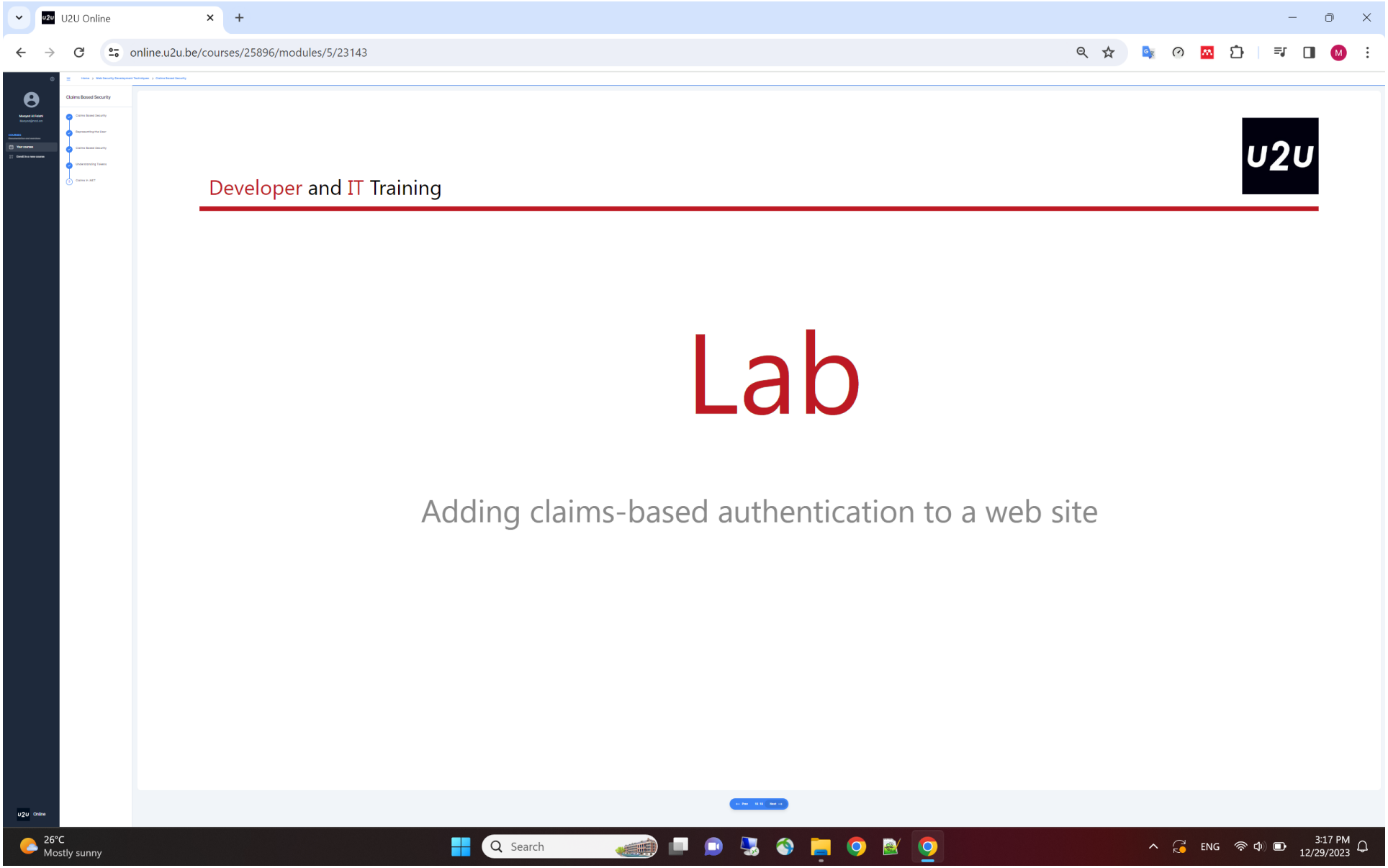

U2U Online
online.u2u.be/courses/25896/modules/5/23143
Some Common Claims
U2U
iss : The identity of the issuer of the token (has to match issuer)
sub: identifier of the subject that went through the authentication process
aud: audience of the token (intended recipient, match to client id)
exp: expiration time of the token
nbf: not before time of the token
iat: the instant at which the token was created, i.e., how old is it?
26°C
Mostly sunny
Search
ENG
3:16 PM
12/29/2023


U2U Online
online.u2u.be/courses/25896/modules/5/23143
IPrincipal and IIdentity
U2U
So how do I get to the claims of the current authenticated user?
Security information is generally stored on the thread
CurrentPrincipal
In ASP.NET MVC also stored in Controller's User property
ClaimsPrincipal claims = this.User;
[ComVisible(true)]
public interface IPrincipal
{
IIdentity Identity { get; }
bool IsInRole(string role);
}
[ComVisible(true)]
public interface IIdentity
{
string AuthenticationType { get; }
bool IsAuthenticated { get; }
string Name { get; }
}
26°C
Mostly sunny
Search
ENG
3:16 PM
12/29/2023


U2U Online
online.u2u.be/courses/25896/modules/5/23143
ClaimsPrincipalSelector
U2U
The ClaimsPrincipal instance is normally stored in either
Thread.CurrentPrincipal
HttpContext.Current.User
However, ClaimsPrincipal also has a delegate: ClaimsPrincipalSelector
Allows you to change where the ClaimsPrincipal is stored
26°C
Mostly sunny
Search
ENG
3:16 PM
12/29/2023


U2U Online
online.u2u.be/courses/25896/modules/5/23143
ClaimsPrincipal
u2u
IPrincipal is an abstraction of the real principal
WindowsPrincipal
GenericPrincipal
ClaimsPrincipal
System.Security.Claims.ClaimsPrincipal is how .NET represents the user
Each claim is represented through the Claim class
A claim is a combination of a ClaimType and a value
Use the ClaimTypes enumeration to look for common attributes
Claim firstName = claims.FindFirst(ClaimTypes.GivenName);
26°C
Mostly sunny
Search
ENG
3:16 PM
12/29/2023


U2U Online
online.u2u.be/courses/25896/modules/5/23143
Claims Based Security
Developer and IT Training
u2u
Demo
Using OAuth/2, OpenID Connect and AzureAD
to protect a website
26°C
Mostly sunny
Search
ENG
3:17 PM
12/29/2023


U2U Online
online.u2u.be/courses/25896/modules/5/23143
Claims Based Security
Developer and IT Training
U2U
Lab
Adding claims-based authentication to a web site
26°C
Mostly sunny
Search
ENG
3:17 PM
12/29/2023