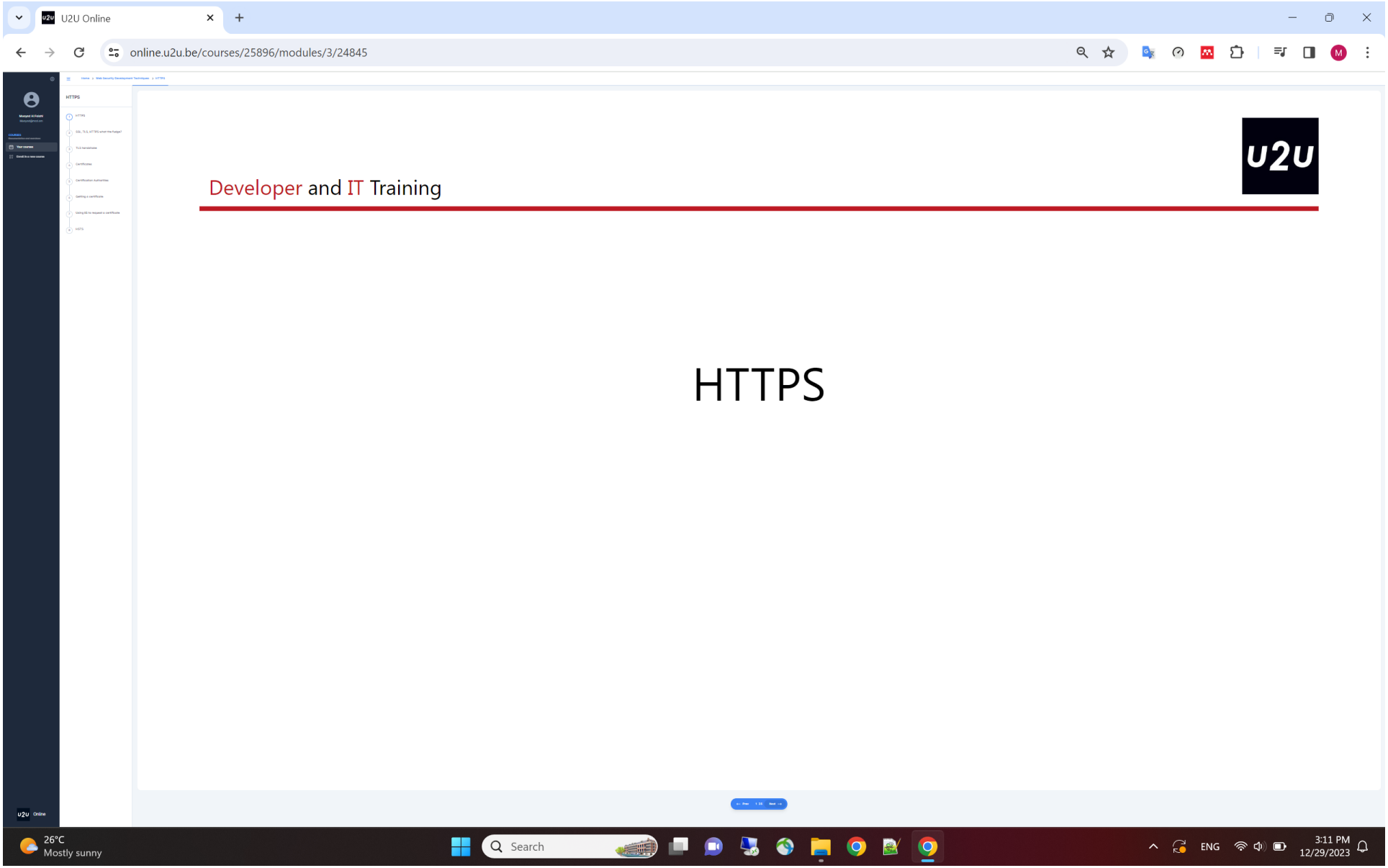
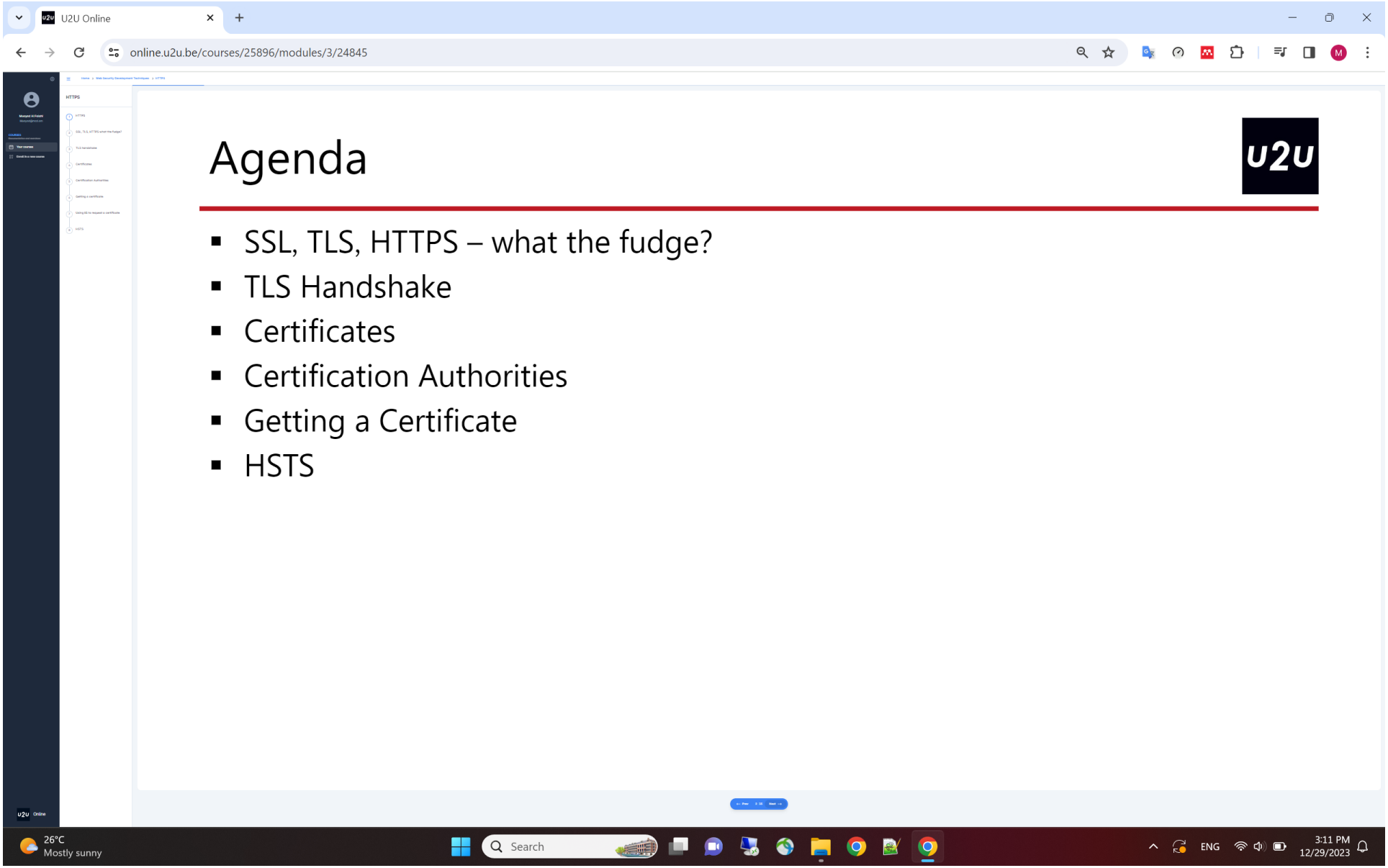
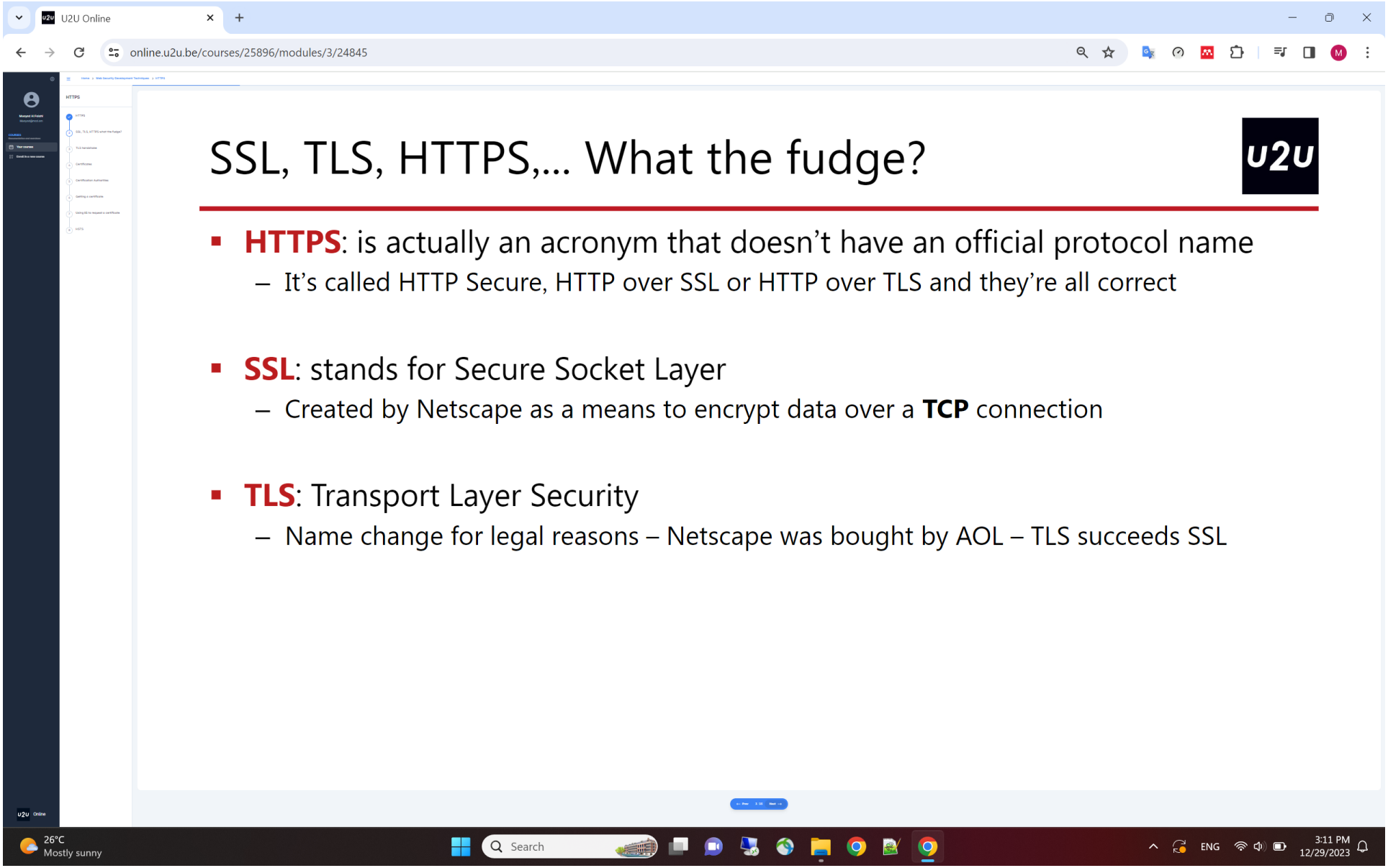
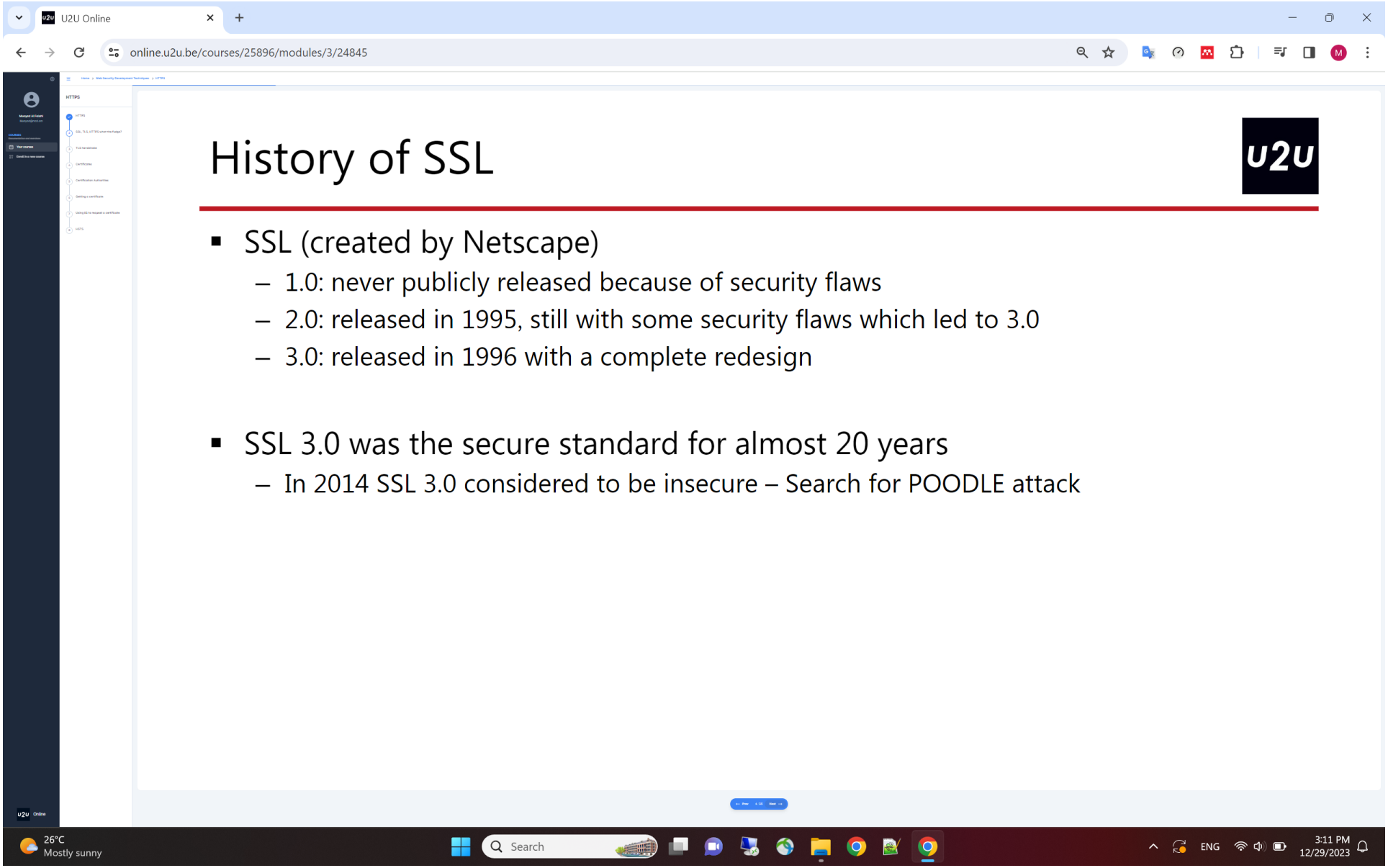
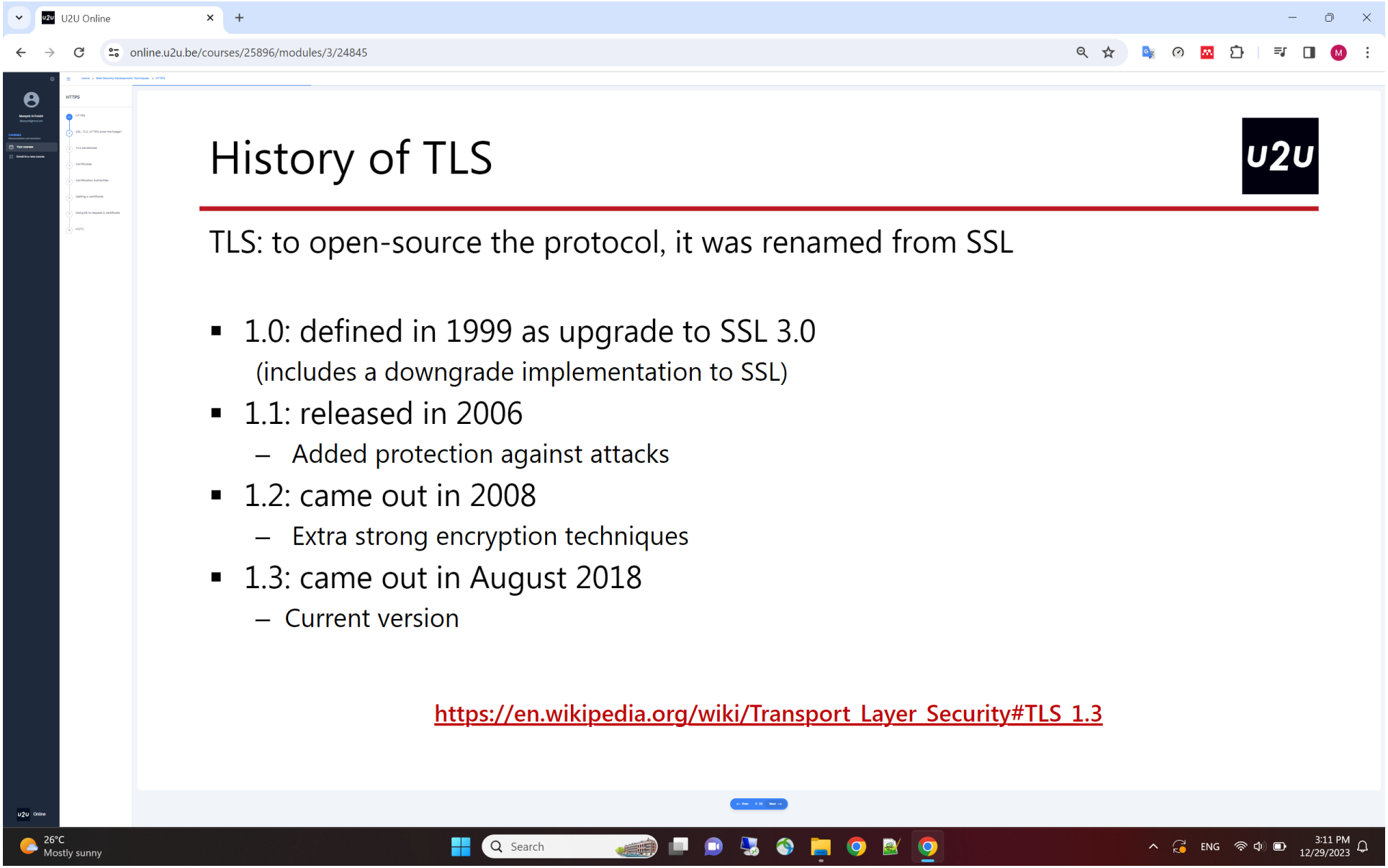
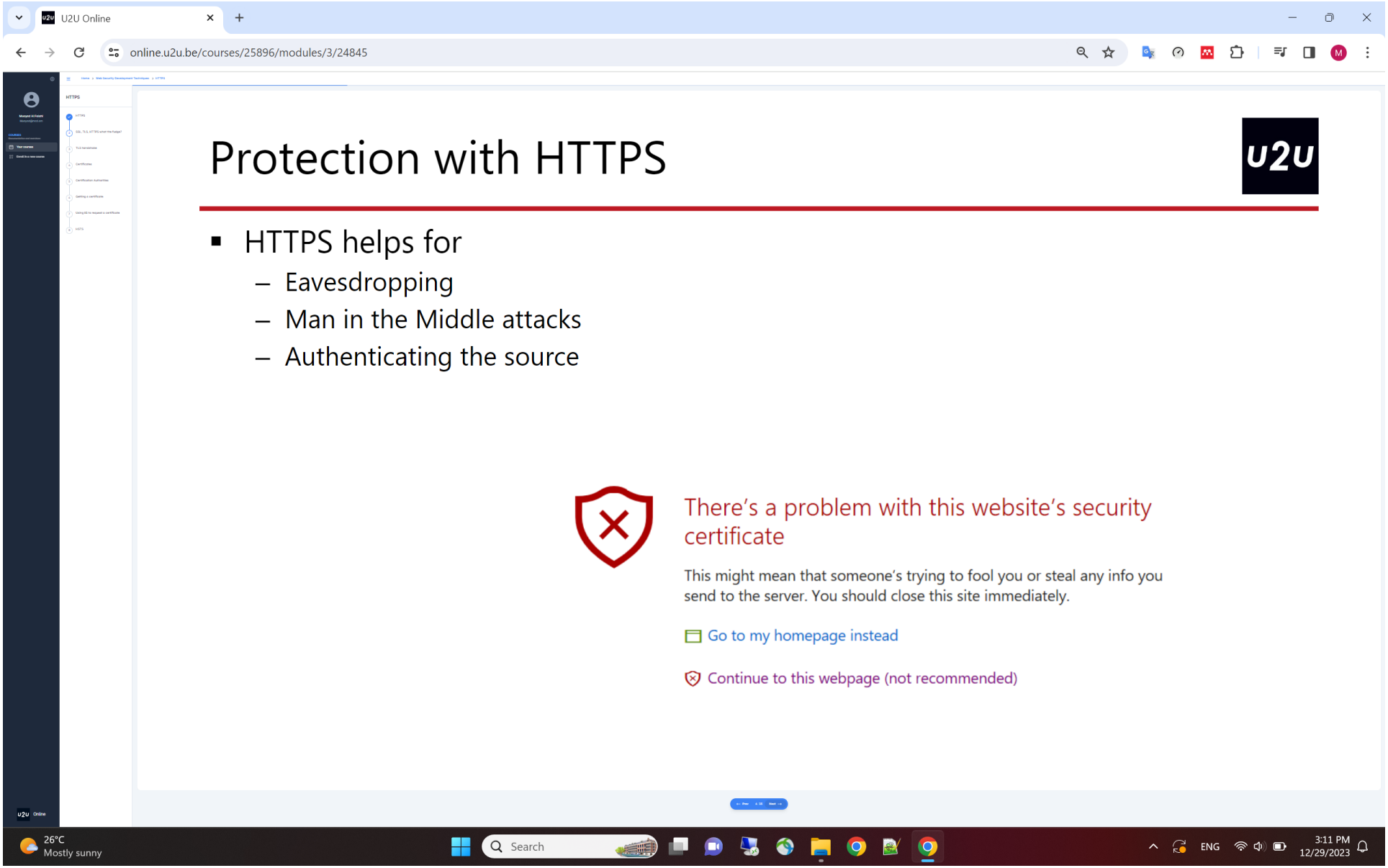

U2U Online
online.u2u.be/courses/25896/modules/3/24845
HTTPS
Developer and IT Training
HTTPS
26°C
Mostly sunny
Search
ENG
3:11 PM
12/29/2023


U2U Online
online.u2u.be/courses/25896/modules/3/24845
HTTPS
Agenda
u2u
SSL, TLS, HTTPS – what the fudge?
TLS Handshake
Certificates
Certification Authorities
Getting a Certificate
HSTS
26°C
Mostly sunny
Search
ENG
3:11 PM
12/29/2023

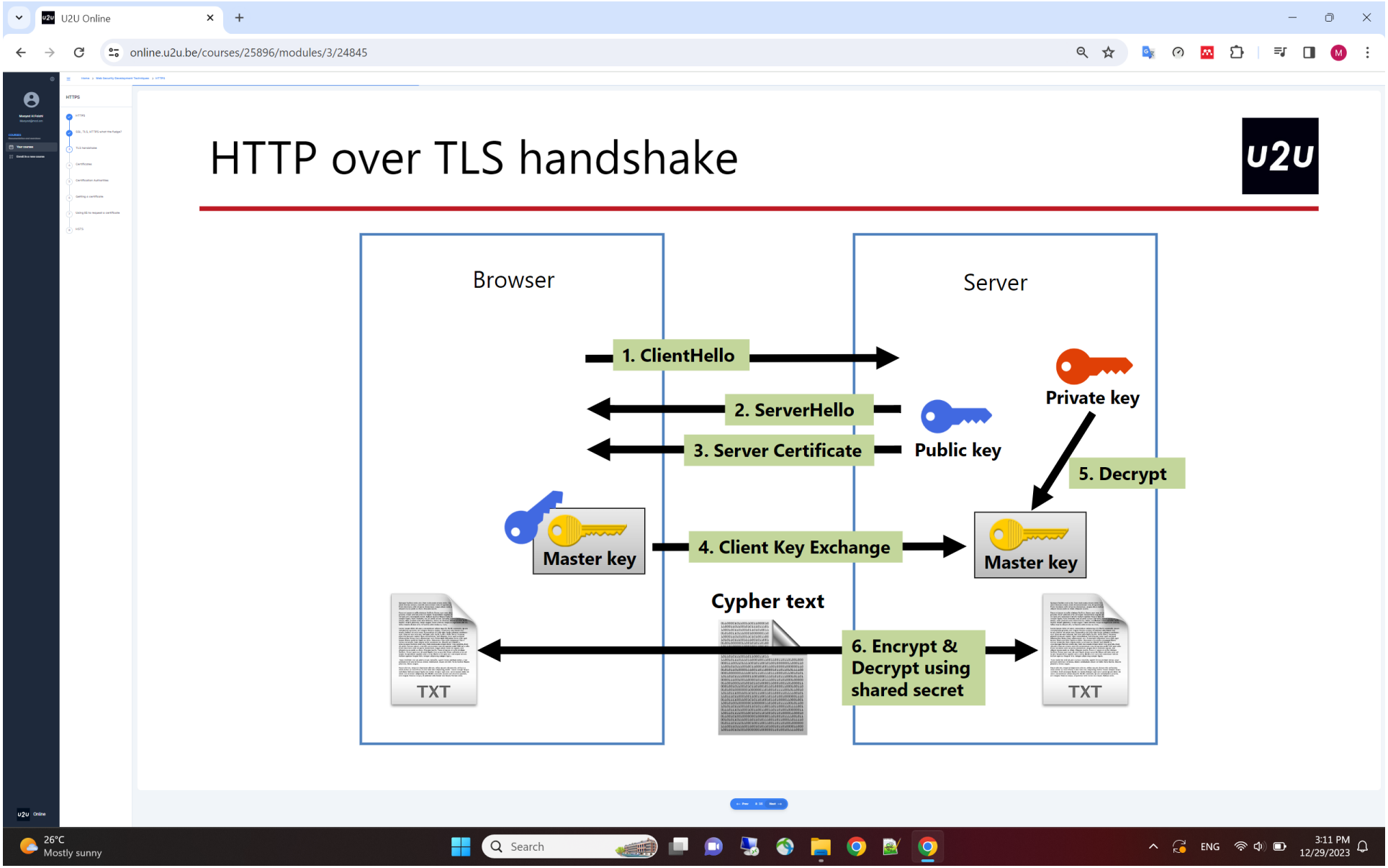

U2U Online
online.u2u.be/courses/25896/modules/3/24845
SSL, TLS, HTTPS,... What the fudge?
U2U
HTTPS: is actually an acronym that doesn't have an official protocol name
It's called HTTP Secure, HTTP over SSL or HTTP over TLS and they're all correct
SSL: stands for Secure Socket Layer
Created by Netscape as a means to encrypt data over a TCP connection
TLS: Transport Layer Security
Name change for legal reasons – Netscape was bought by AOL – TLS succeeds SSL
26°C
Mostly sunny
Search
ENG
3:11 PM
12/29/2023

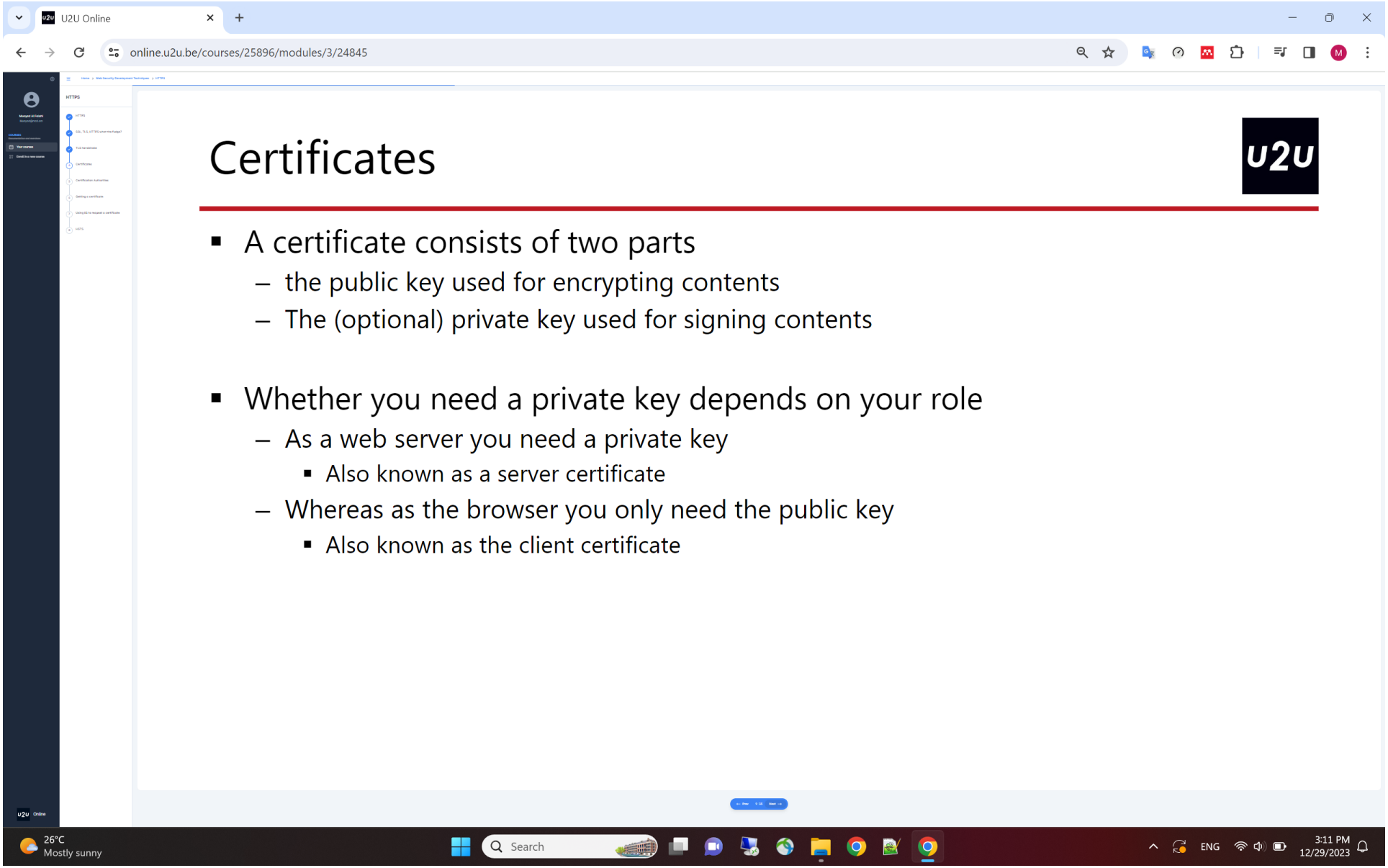

U2U Online
online.u2u.be/courses/25896/modules/3/24845
HTTPS
History of SSL
U2U
SSL (created by Netscape)
1.0: never publicly released because of security flaws
2.0: released in 1995, still with some security flaws which led to 3.0
3.0: released in 1996 with a complete redesign
SSL 3.0 was the secure standard for almost 20 years
In 2014 SSL 3.0 considered to be insecure – Search for POODLE attack
26°C
Mostly sunny
Search
ENG
3:11 PM
12/29/2023

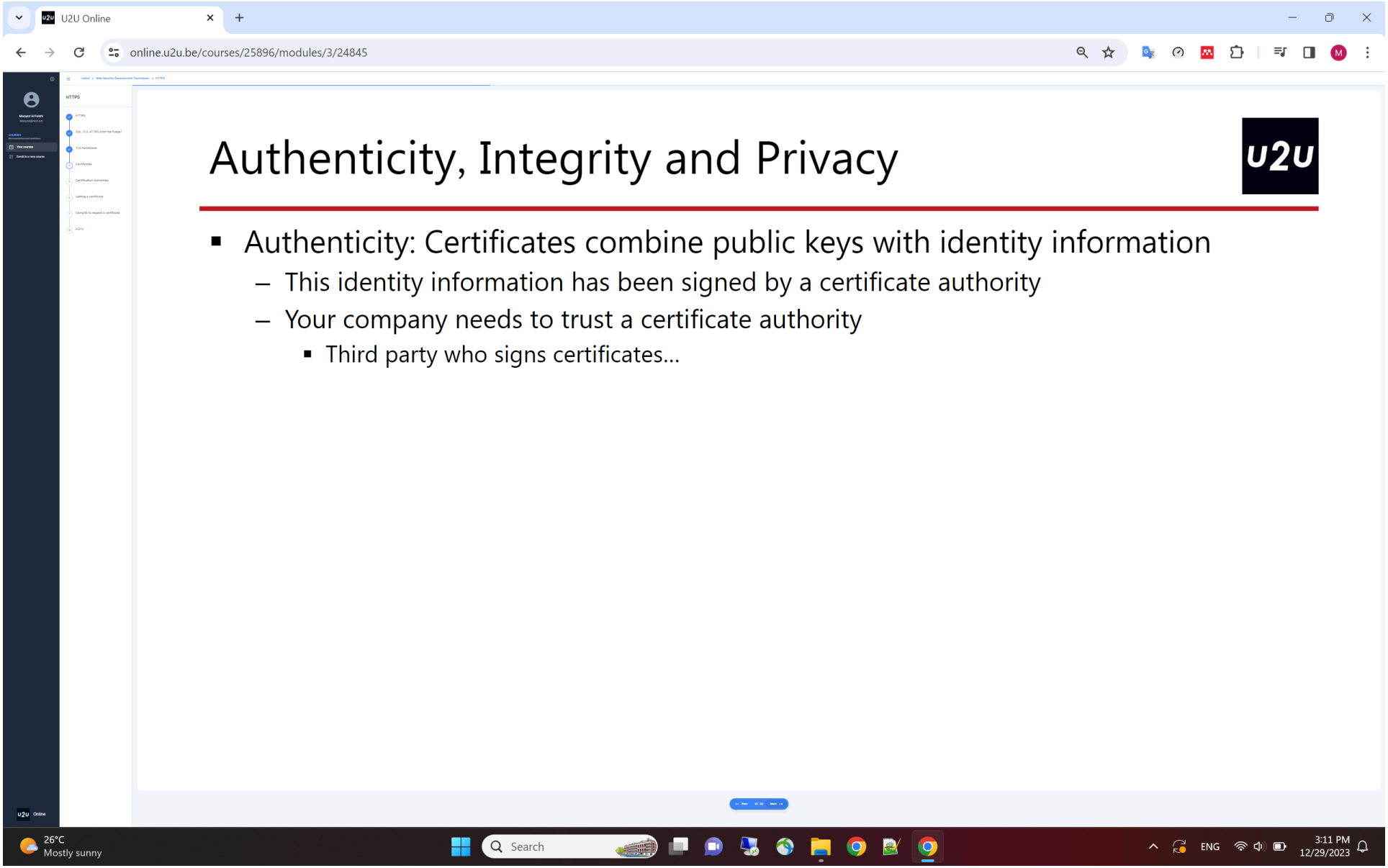

U2U Online
online.u2u.be/courses/25896/modules/3/24845
HTTPS
History of TLS
U2U
TLS: to open-source the protocol, it was renamed from SSL
1.0: defined in 1999 as upgrade to SSL 3.0
(includes a downgrade implementation to SSL)
1.1: released in 2006
– Added protection against attacks
1.2: came out in 2008
– Extra strong encryption techniques
1.3: came out in August 2018
– Current version
https://en.wikipedia.org/wiki/Transport_Layer_Security#TLS_1.3
26°C
Mostly sunny
Search
ENG
3:11 PM
12/29/2023


U2U Online
online.u2u.be/courses/25896/modules/3/24845
Protection with HTTPS
U2U
HTTPS helps for
Eavesdropping
Man in the Middle attacks
Authenticating the source
There's a problem with this website's security certificate
This might mean that someone's trying to fool you or steal any info you send to the server. You should close this site immediately.
Go to my homepage instead
Continue to this webpage (not recommended)
26°C
Mostly sunny
Search
ENG
3:11 PM
12/29/2023


U2U Online
online.u2u.be/courses/25896/modules/3/24845
TLS Handshake
u2u
TLS uses a certificate to start a new secure connection
It is an implementation of a Hybrid Encryption technique
Symmetric encryption
Key generated by the client
Asymmetric encryption
Certificate(s)
26°C
Mostly sunny
Search
ENG
3:11 PM
12/29/2023


U2U Online
online.u2u.be/courses/25896/modules/3/24845
HTTP over TLS handshake
u2u
Browser
Server
1. ClientHello
2. ServerHello
3. Server Certificate
Public key
Private key
5. Decrypt
Master key
4. Client Key Exchange
Master key
Cypher text
TXT
6. Encrypt & Decrypt using shared secret
TXT
26°C
Mostly sunny
Search
ENG
3:11 PM
12/29/2023


U2U Online
online.u2u.be/courses/25896/modules/3/24845
HTTPS
Certificates
u2u
A certificate consists of two parts
the public key used for encrypting contents
The (optional) private key used for signing contents
Whether you need a private key depends on your role
As a web server you need a private key
Also known as a server certificate
Whereas as the browser you only need the public key
Also known as the client certificate
26°C
Mostly sunny
Search
ENG
3:11 PM
12/29/2023

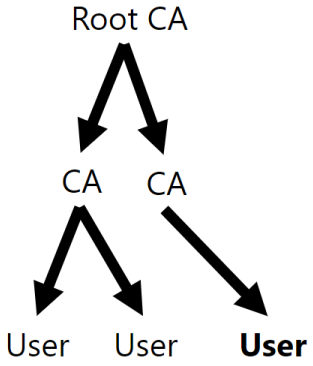

U2U Online
online.u2u.be/courses/25896/modules/3/24845
Authenticity, Integrity and Privacy
U2U
Authenticity: Certificates combine public keys with identity information
This identity information has been signed by a certificate authority
Your company needs to trust a certificate authority
Third party who signs certificates…
26°C
Mostly sunny
Search
ENG
3:11 PM
12/29/2023

U2U Online

online.u2u.be/courses/25896/modules/3/24845

Certificate Authorities

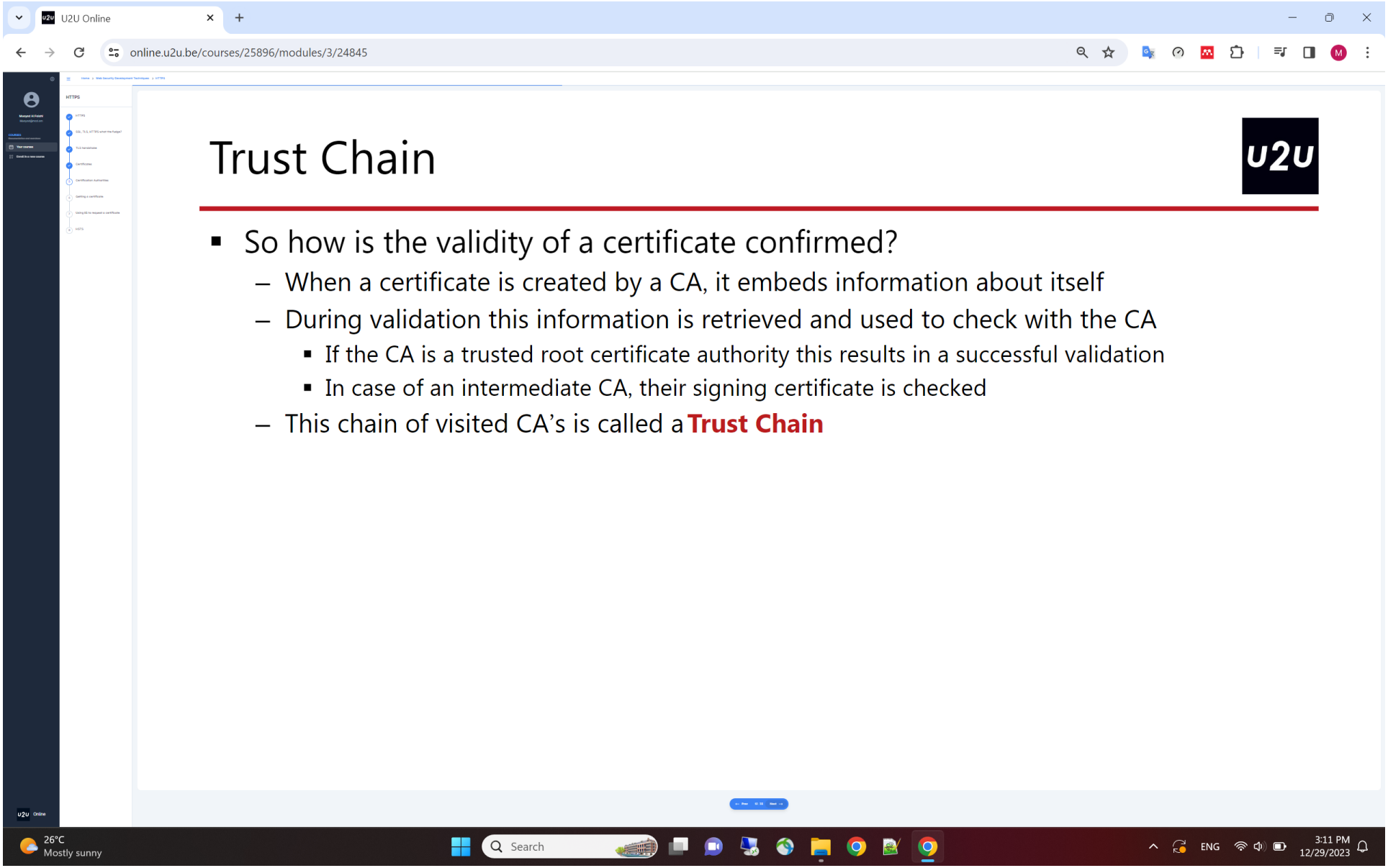
- Certificates are signed by certificate authorities
  - But how do I know if I can trust a certificate authority?
- Root certificate authorities
  - Carry the highest trust
  - E.g. Thawte, Verisign, …
- Intermediate certificate authorities



26°C Mostly sunny

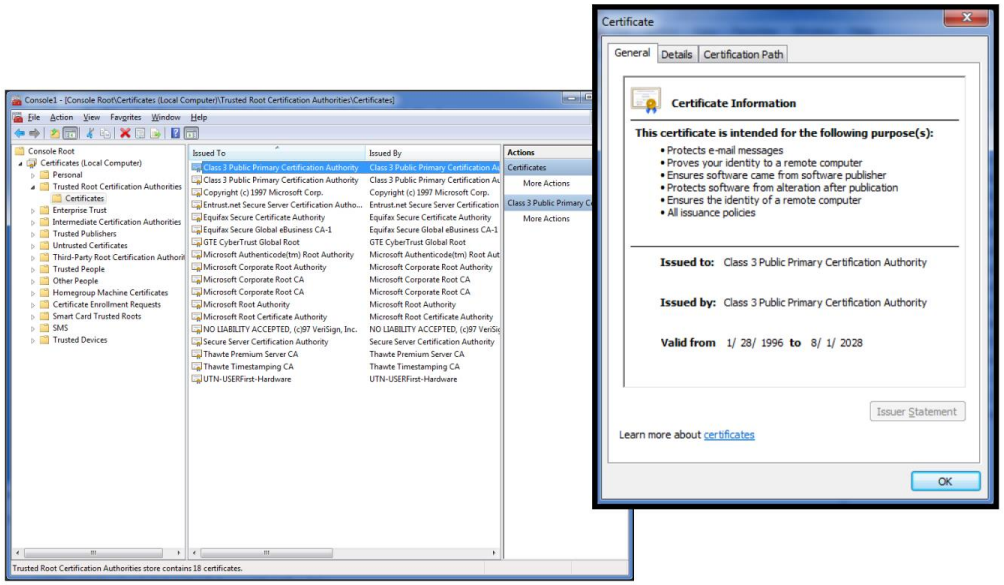
Search

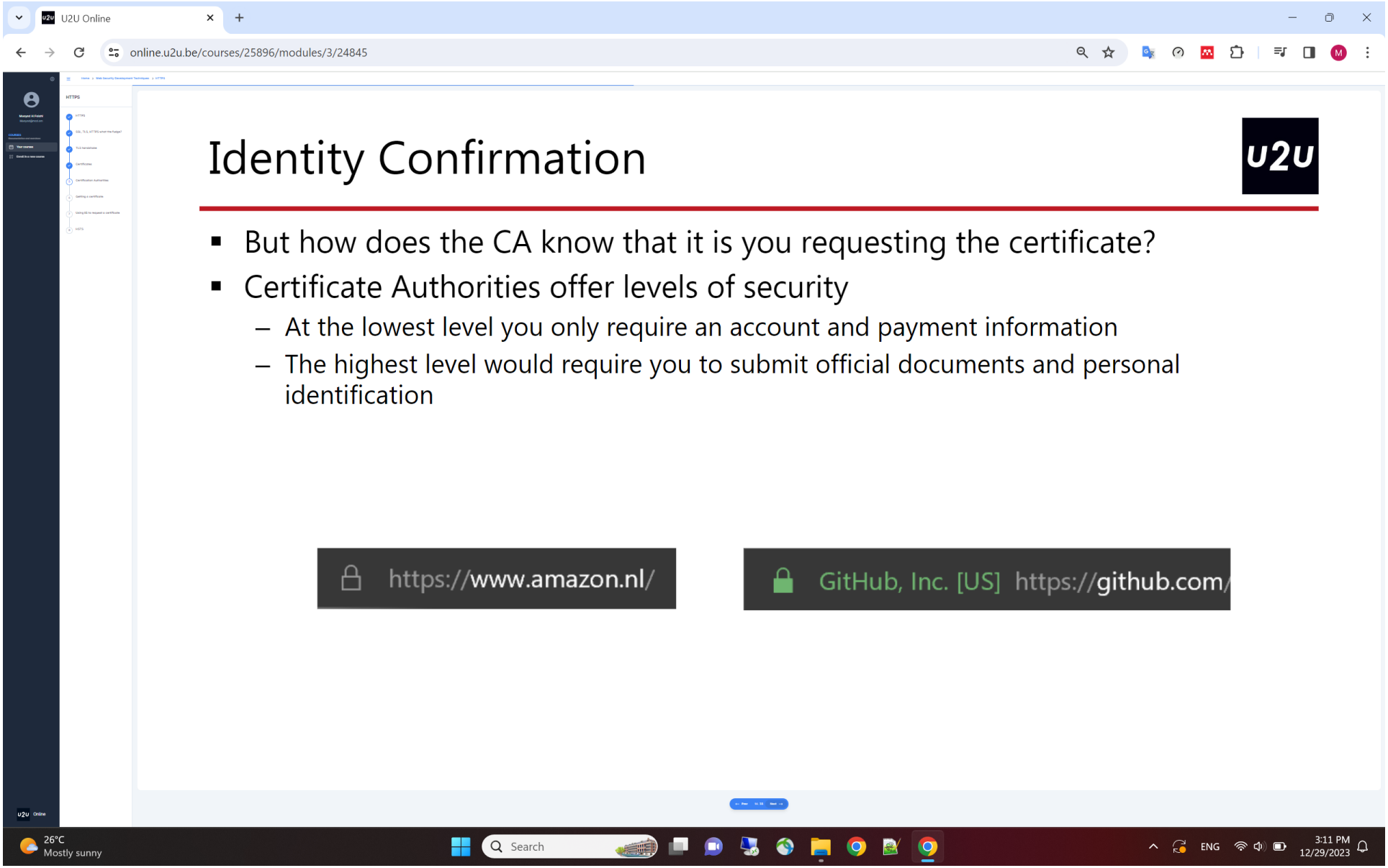
ENG 3:11 PM 12/29/2023

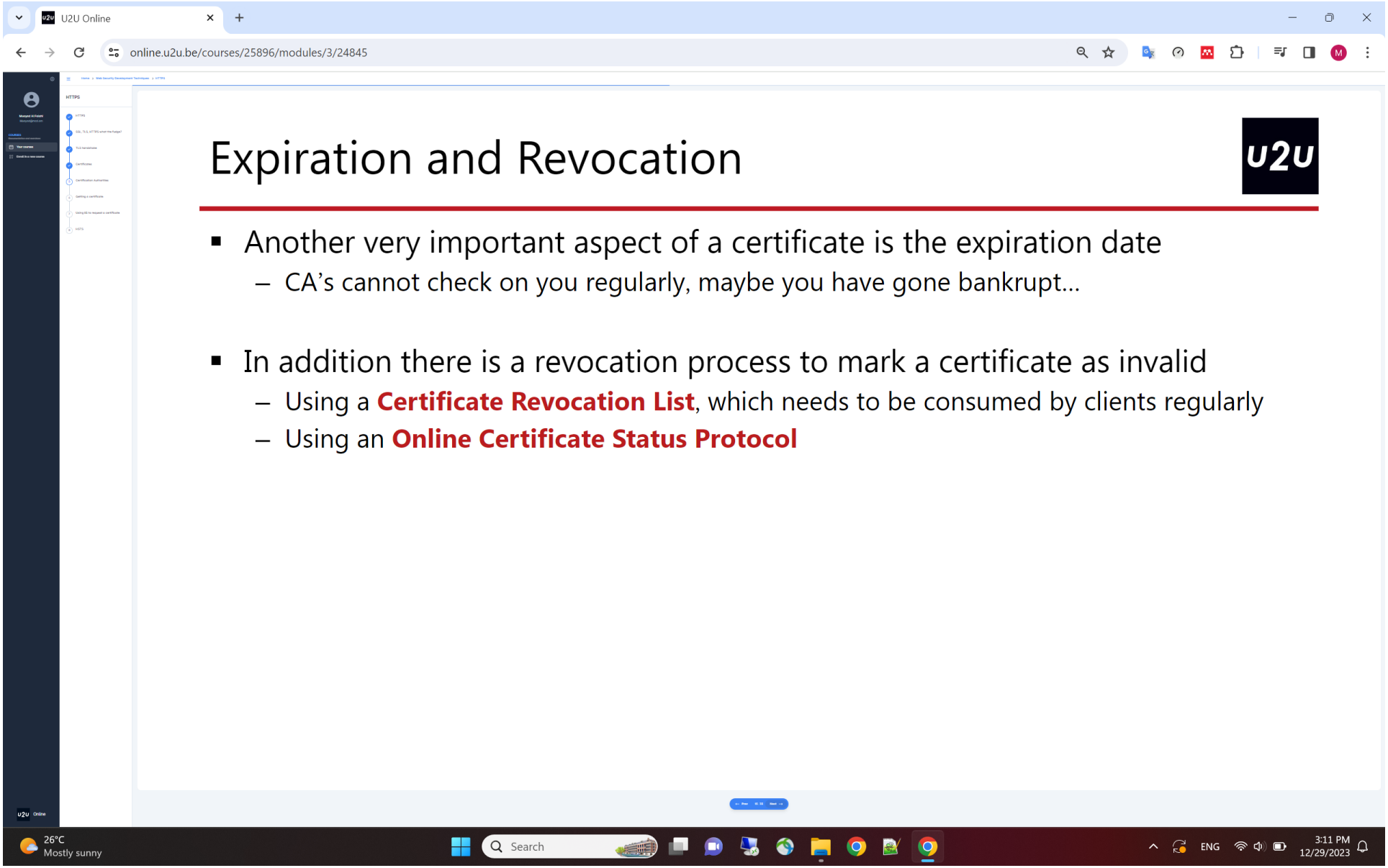

U2U Online
online.u2u.be/courses/25896/modules/3/24845
HTTPS
Trust Chain
U2U
So how is the validity of a certificate confirmed?
When a certificate is created by a CA, it embeds information about itself
During validation this information is retrieved and used to check with the CA
If the CA is a trusted root certificate authority this results in a successful validation
In case of an intermediate CA, their signing certificate is checked
This chain of visited CA's is called a Trust Chain
26°C
Mostly sunny
Search
ENG
3:11 PM
12/29/2023

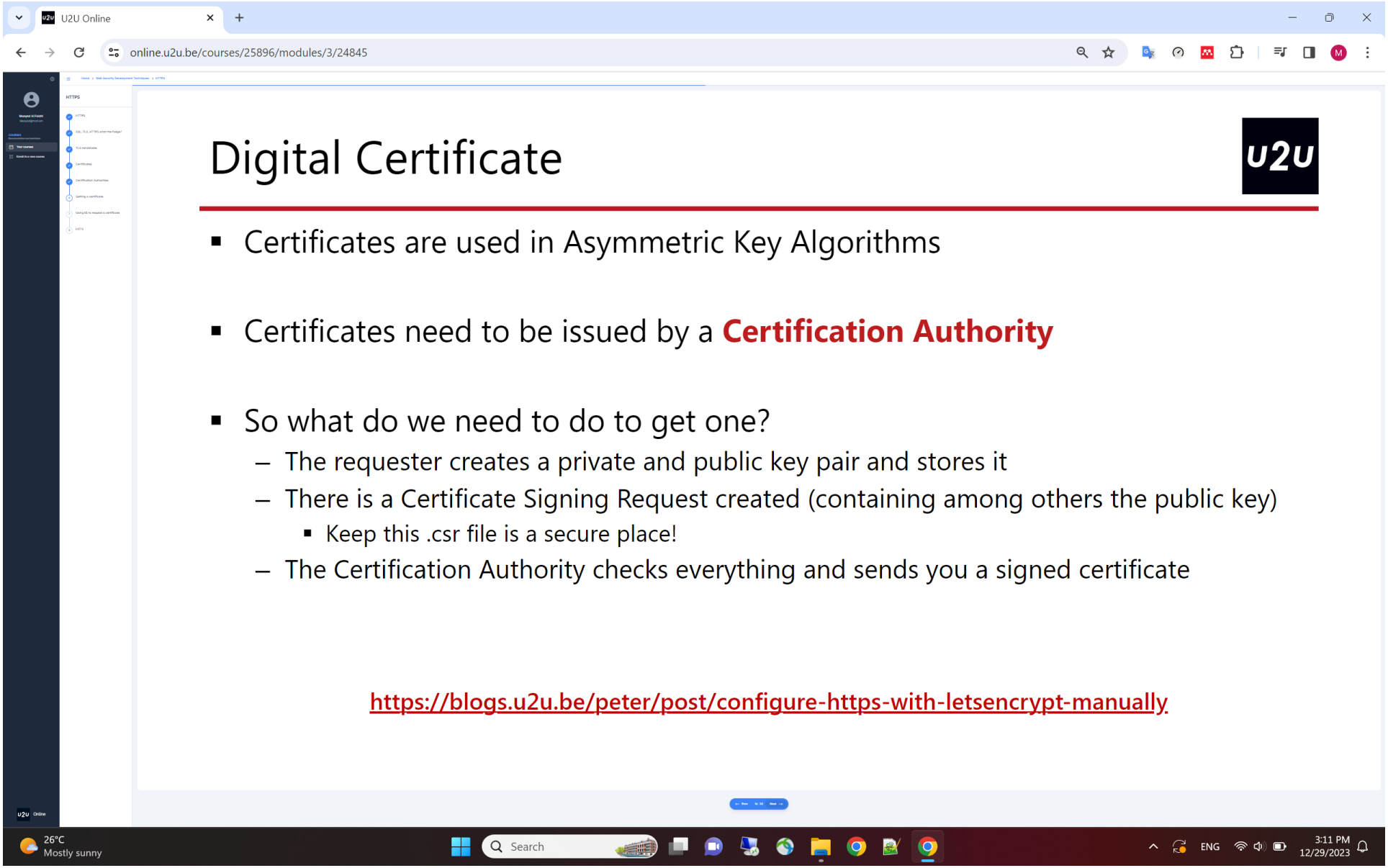
Certificate Checks

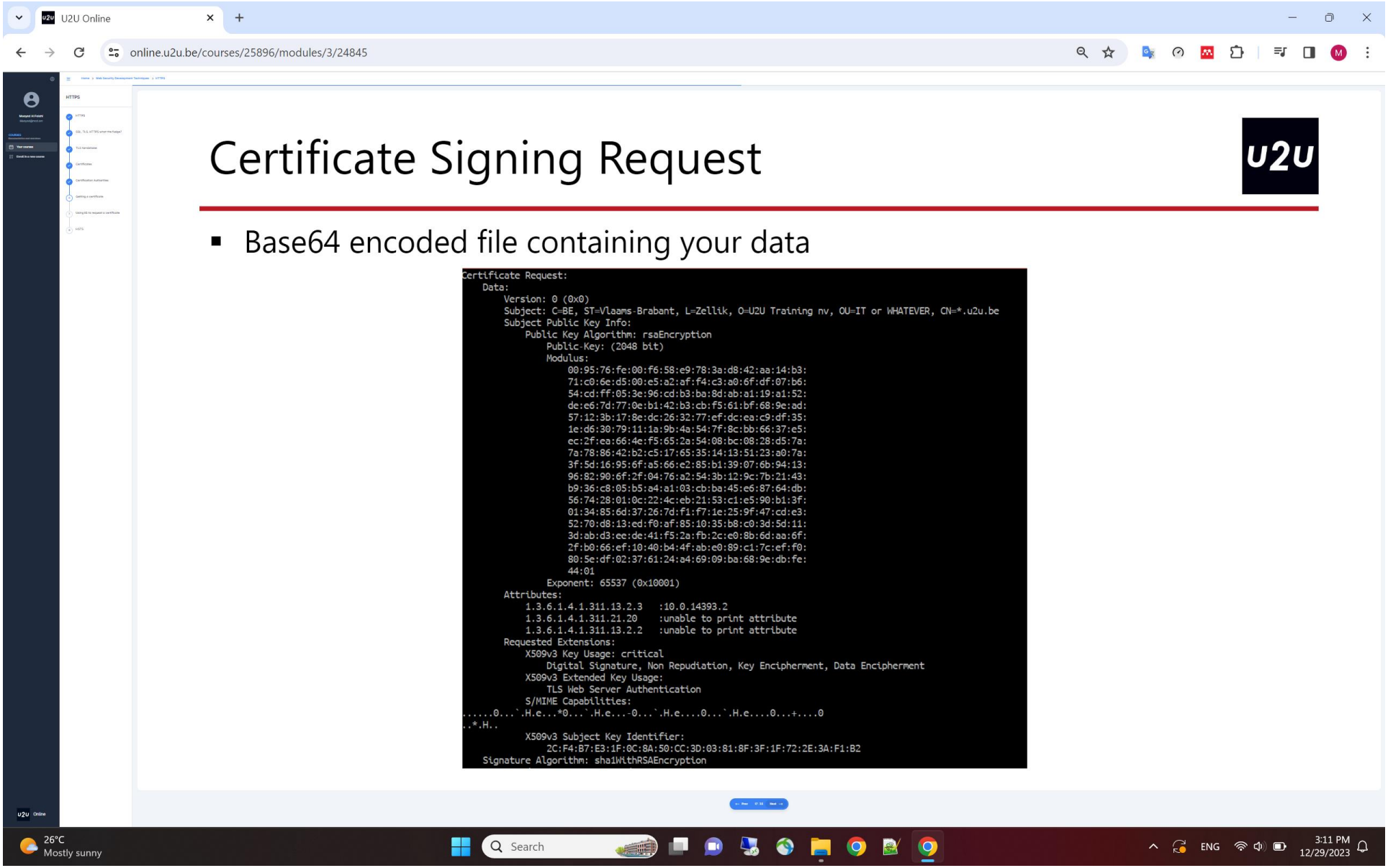
- Trusted Root Certificates
  - The CA that signed a certificate must be in the trusted root certification authorities list




U2U Online
online.u2u.be/courses/25896/modules/3/24845
Identity Confirmation
U2U
But how does the CA know that it is you requesting the certificate?
Certificate Authorities offer levels of security
At the lowest level you only require an account and payment information
The highest level would require you to submit official documents and personal identification
https://www.amazon.nl/
GitHub, Inc. [US] https://github.com/
26°C
Mostly sunny
Search
ENG
3:11 PM
12/29/2023

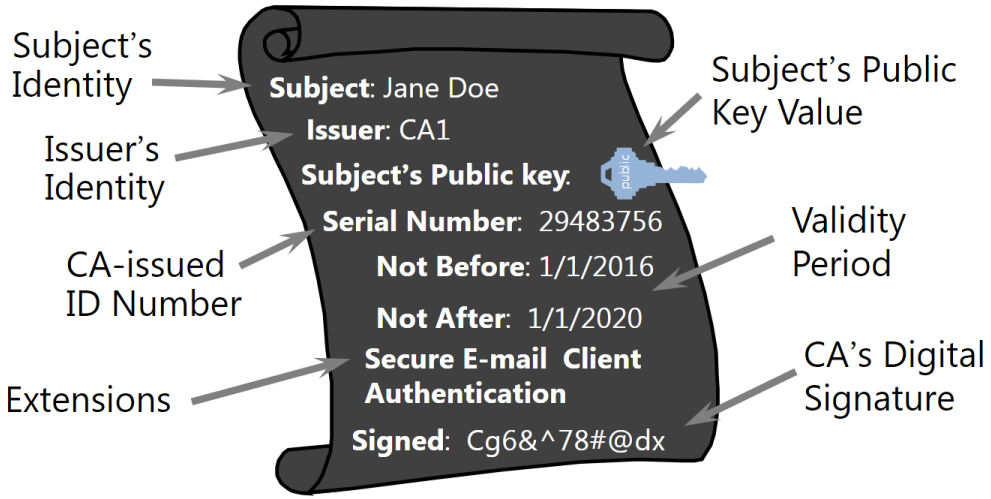

U2U Online
online.u2u.be/courses/25896/modules/3/24845
HTTPS
Expiration and Revocation
u2u
Another very important aspect of a certificate is the expiration date
CA's cannot check on you regularly, maybe you have gone bankrupt…
In addition there is a revocation process to mark a certificate as invalid
Using a Certificate Revocation List, which needs to be consumed by clients regularly
Using an Online Certificate Status Protocol
26°C
Mostly sunny
Search
ENG
3:11 PM
12/29/2023

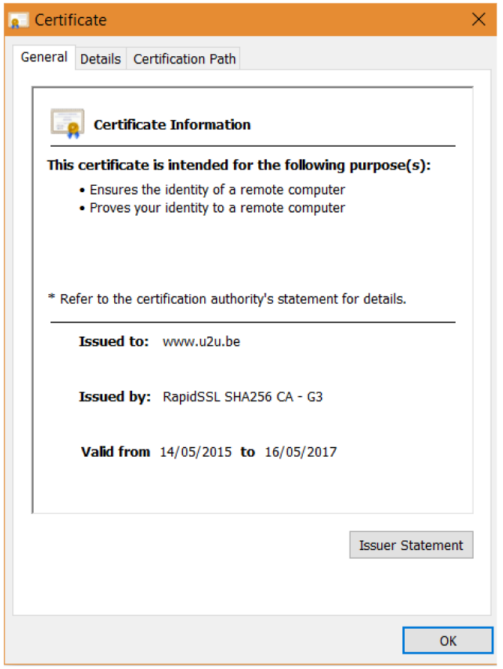

U2U Online
online.u2u.be/courses/25896/modules/3/24845
HTTPS
Digital Certificate
u2u
Certificates are used in Asymmetric Key Algorithms
Certificates need to be issued by a Certification Authority
So what do we need to do to get one?
The requester creates a private and public key pair and stores it
There is a Certificate Signing Request created (containing among others the public key)
Keep this .csr file is a secure place!
The Certification Authority checks everything and sends you a signed certificate
https://blogs.u2u.be/peter/post/configure-https-with-letsencrypt-manually
26°C
Mostly sunny
Search
ENG
3:11 PM
12/29/2023

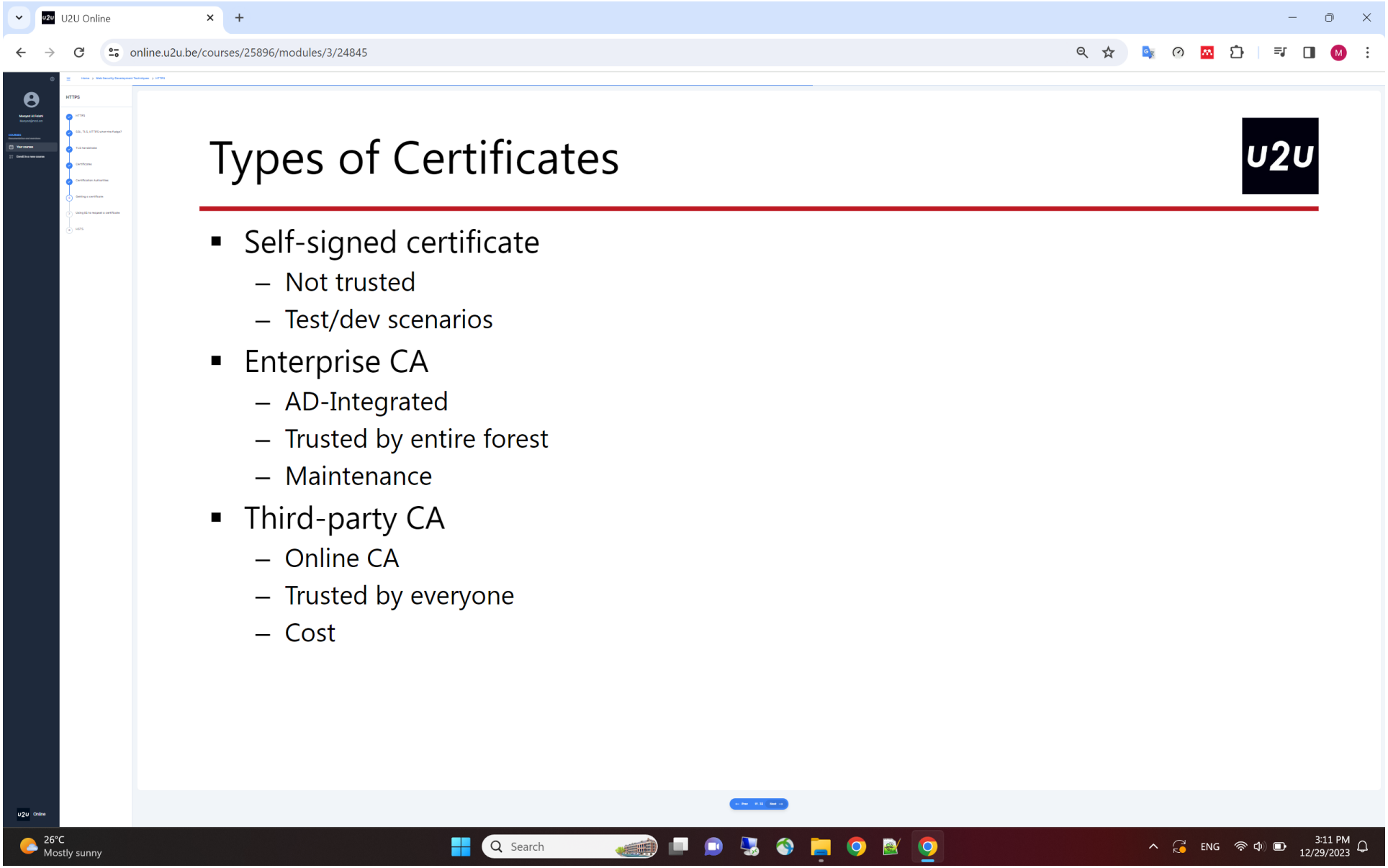

U2U Online
online.u2u.be/courses/25896/modules/3/24845
HTTPS
Certificate Signing Request
u2u
Base64 encoded file containing your data
Certificate Request:
Data:
Version: 0 (0x0)
Subject: C=BE, ST=Vlaams-Brabant, L=Zellik, O=U2U Training nv, OU=IT or WHATEVER, CN=*.u2u.be
Subject Public Key Info:
Public Key Algorithm: rsaEncryption
Public-Key: (2048 bit)
Modulus:
00:95:76:fe:00:f6:58:e9:78:3a:d8:42:aa:14:b3:
71:c0:6e:d5:00:e5:a2:af:f4:c3:a0:6f:df:07:b6:
54:cd:ff:05:3e:96:cd:b3:ba:8d:ab:a1:19:a1:52:
de:e6:7d:77:0e:b1:42:b3:cb:f5:61:bf:68:9e:ad:
57:12:3b:17:8e:dc:26:32:77:ef:dc:ea:c9:df:35:
1e:d6:30:79:11:1a:9b:4a:54:7f:8c:bb:66:37:e5:
ec:2f:ea:66:4e:f5:65:2a:54:08:bc:08:28:d5:7a:
7a:78:86:42:b2:c5:17:65:35:14:13:51:23:a0:7a:
3f:5d:16:95:6f:a5:66:e2:85:b1:39:07:6b:94:13:
96:82:90:6f:2f:04:76:a2:54:3b:12:9c:7b:21:43:
b9:36:c8:05:b5:a4:a1:03:cb:ba:45:e6:87:64:db:
56:74:28:01:0c:22:4c:eb:21:53:c1:e5:90:b1:3f:
01:34:85:6d:37:26:7d:f1:f7:1e:25:9f:47:cd:e3:
52:70:d8:13:ed:f0:af:85:10:35:b8:c0:3d:5d:11:
3d:ab:d3:ee:de:41:f5:2a:fb:2c:e0:8b:6d:aa:6f:
2f:b0:66:ef:10:40:b4:4f:ab:e0:89:c1:7c:ef:f0:
80:5e:df:02:37:61:24:a4:69:09:ba:68:9e:db:fe:
44:01
Exponent: 65537 (0x10001)
Attributes:
1.3.6.1.4.1.311.13.2.3 :10.0.14393.2
1.3.6.1.4.1.311.21.20 :unable to print attribute
1.3.6.1.4.1.311.13.2.2 :unable to print attribute
Requested Extensions:
X509v3 Key Usage: critical
Digital Signature, Non Repudiation, Key Encipherment, Data Encipherment
X509v3 Extended Key Usage:
TLS Web Server Authentication
S/MIME Capabilities:
.....0...`.H.e...*0...`.H.e...-0...`.H.e....0...`.H.e....0...+....0
..*.H..
X509v3 Subject Key Identifier:
2C:F4:B7:E3:1F:0C:8A:50:CC:3D:03:81:8F:3F:1F:72:2E:3A:F1:B2
Signature Algorithm: sha1WithRSAEncryption
26°C
Mostly sunny
Search
ENG
3:11 PM
12/29/2023

Digital Certificate

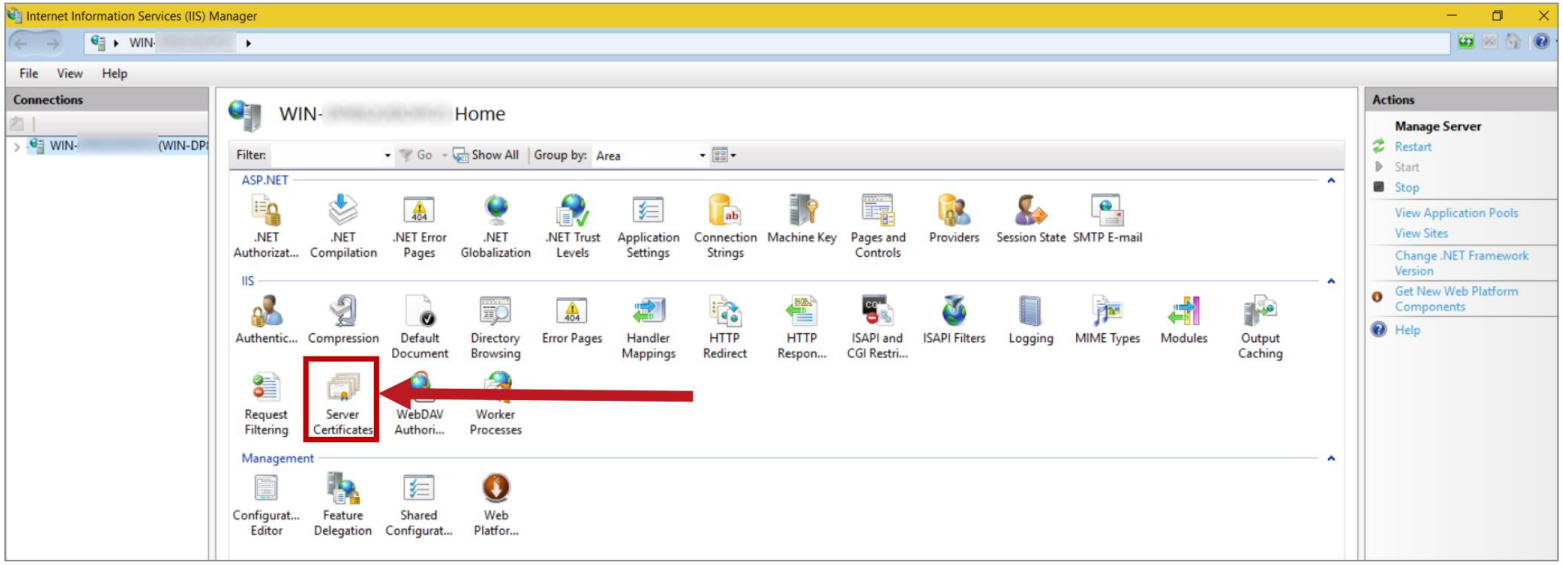
- Links the subject's identity to a public key
  - Signed by a certification authority (CA)

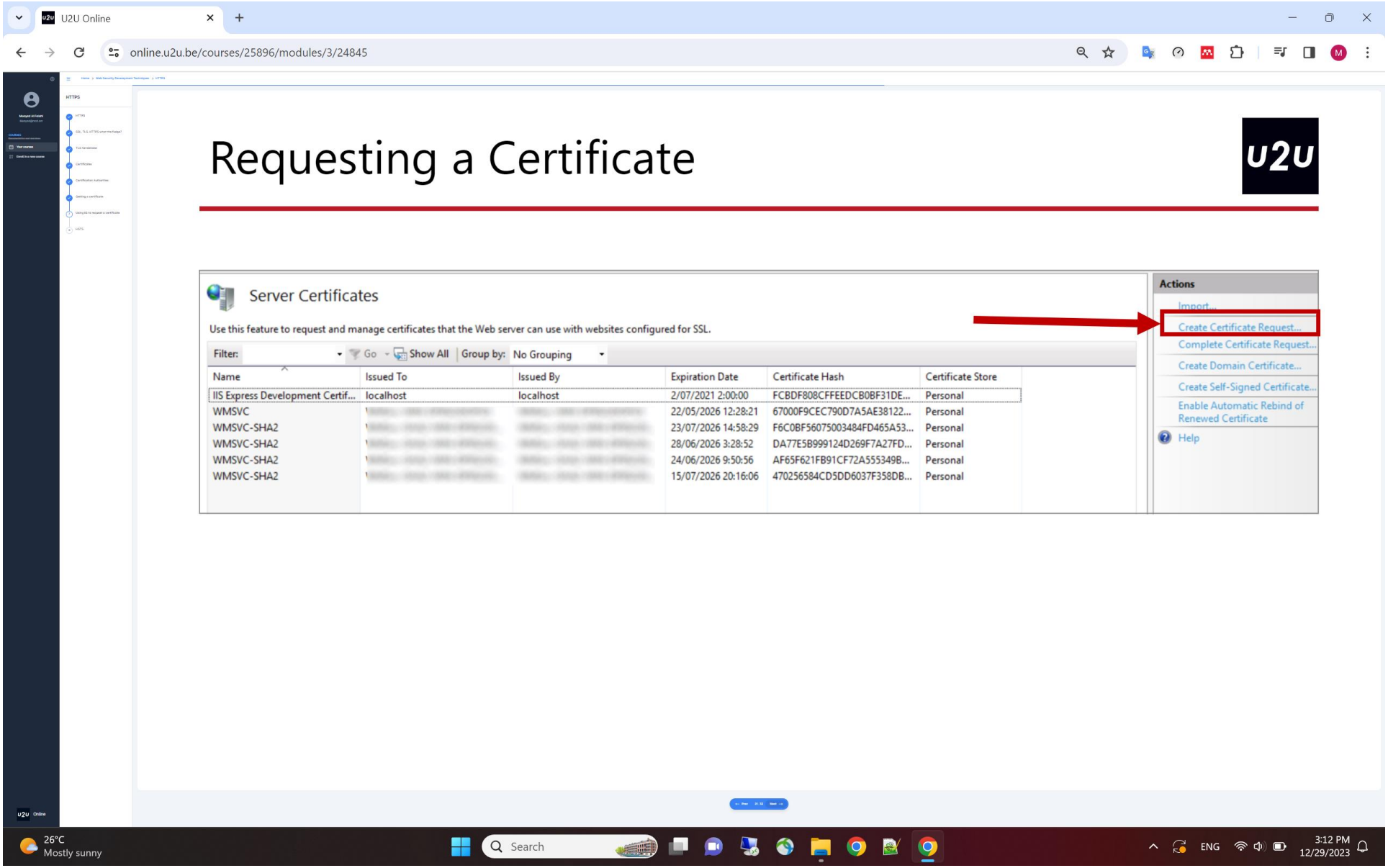


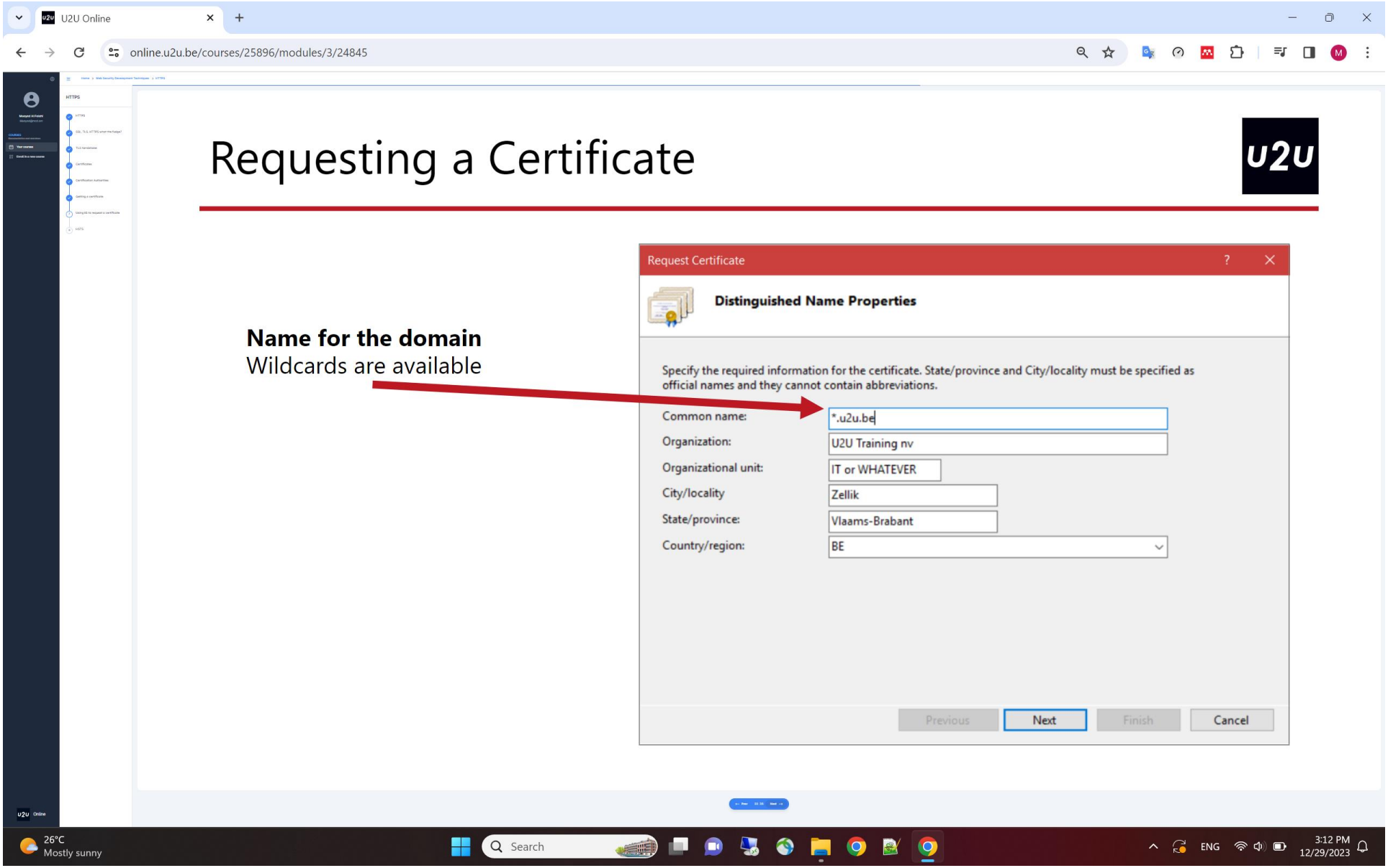


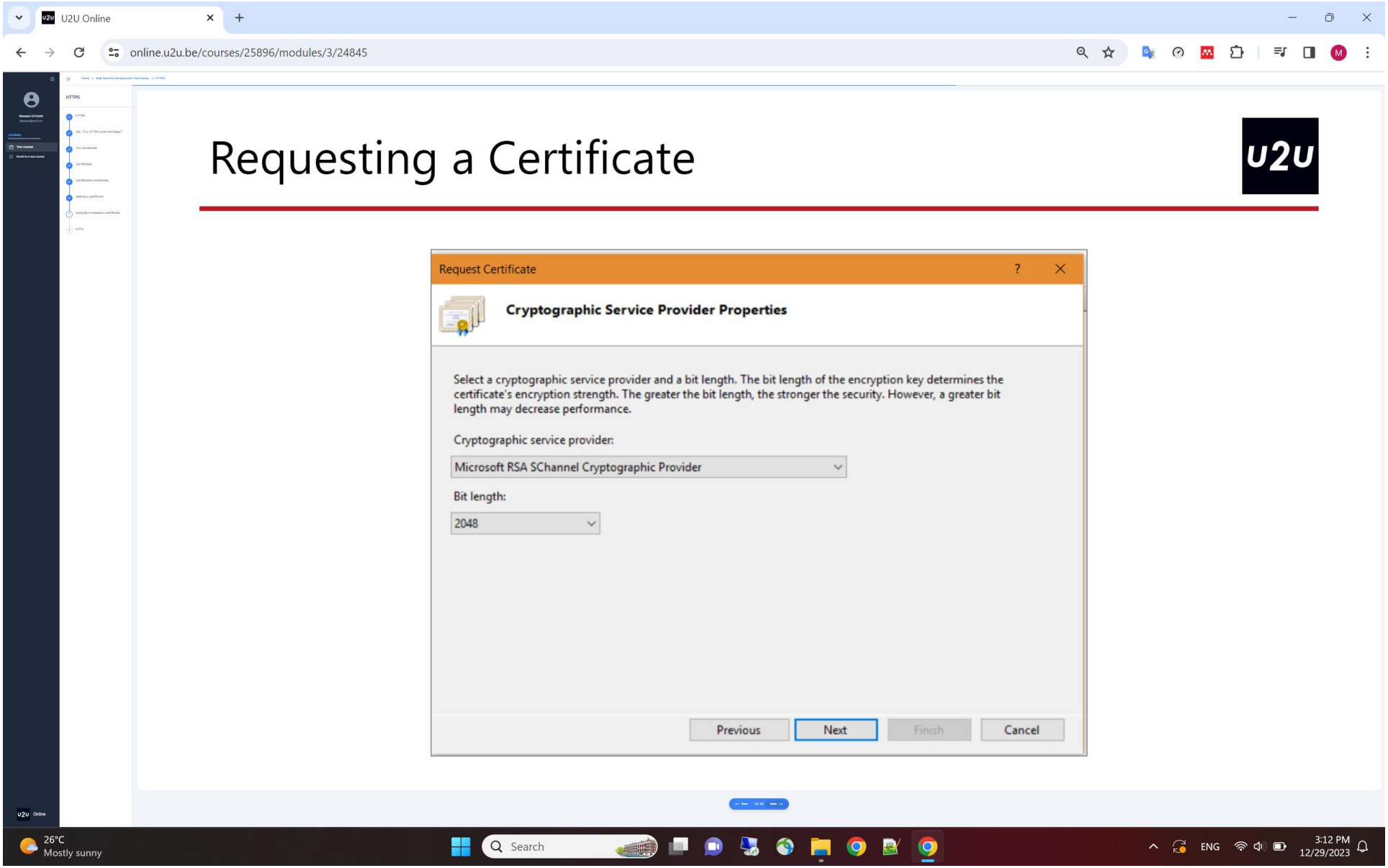

U2U Online
online.u2u.be/courses/25896/modules/3/24845
HTTPS
Types of Certificates
U2U
Self-signed certificate
Not trusted
Test/dev scenarios
Enterprise CA
AD-Integrated
Trusted by entire forest
Maintenance
Third-party CA
Online CA
Trusted by everyone
Cost
26°C
Mostly sunny
Search
ENG
3:11 PM
12/29/2023

Requesting a Certificate



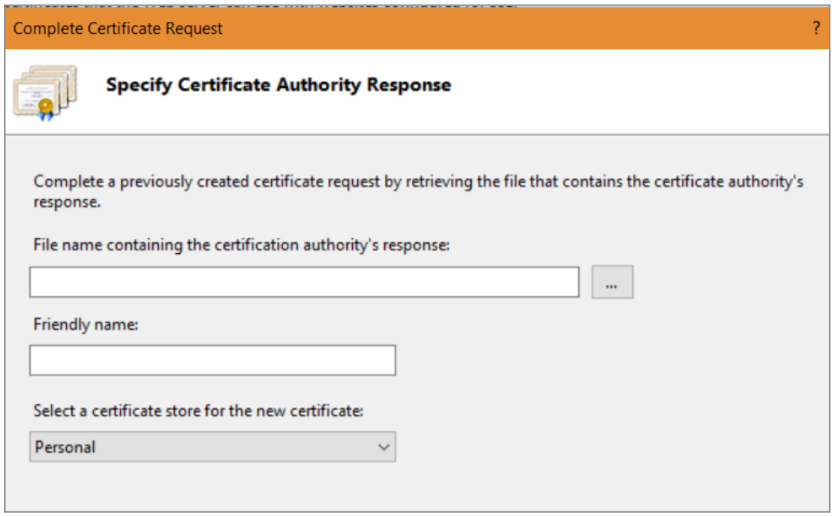

U2U Online
online.u2u.be/courses/25896/modules/3/24845
Requesting a Certificate
u2u
Server Certificates
Use this feature to request and manage certificates that the Web server can use with websites configured for SSL.
Filter:
Go
Show All
Group by:
No Grouping
Name
Issued To
Issued By
Expiration Date
Certificate Hash
Certificate Store
IIS Express Development Certif...
localhost
localhost
2/07/2021 2:00:00
FCBDF808CFFEEDCB0BF31DE...
Personal
WMSVC
22/05/2026 12:28:21
67000F9CEC790D7A5AE38122...
Personal
WMSVC-SHA2
23/07/2026 14:58:29
F6C0BF56075003484FD465A53...
Personal
WMSVC-SHA2
28/06/2026 3:28:52
DA77E5B999124D269F7A27FD...
Personal
WMSVC-SHA2
24/06/2026 9:50:56
AF65F621FB91CF72A555349B...
Personal
WMSVC-SHA2
15/07/2026 20:16:06
470256584CD5DD6037F358DB...
Personal
Actions
Import...
Create Certificate Request...
Complete Certificate Request...
Create Domain Certificate...
Create Self-Signed Certificate...
Enable Automatic Rebind of Renewed Certificate
Help
26°C
Mostly sunny
Search
ENG
3:12 PM
12/29/2023

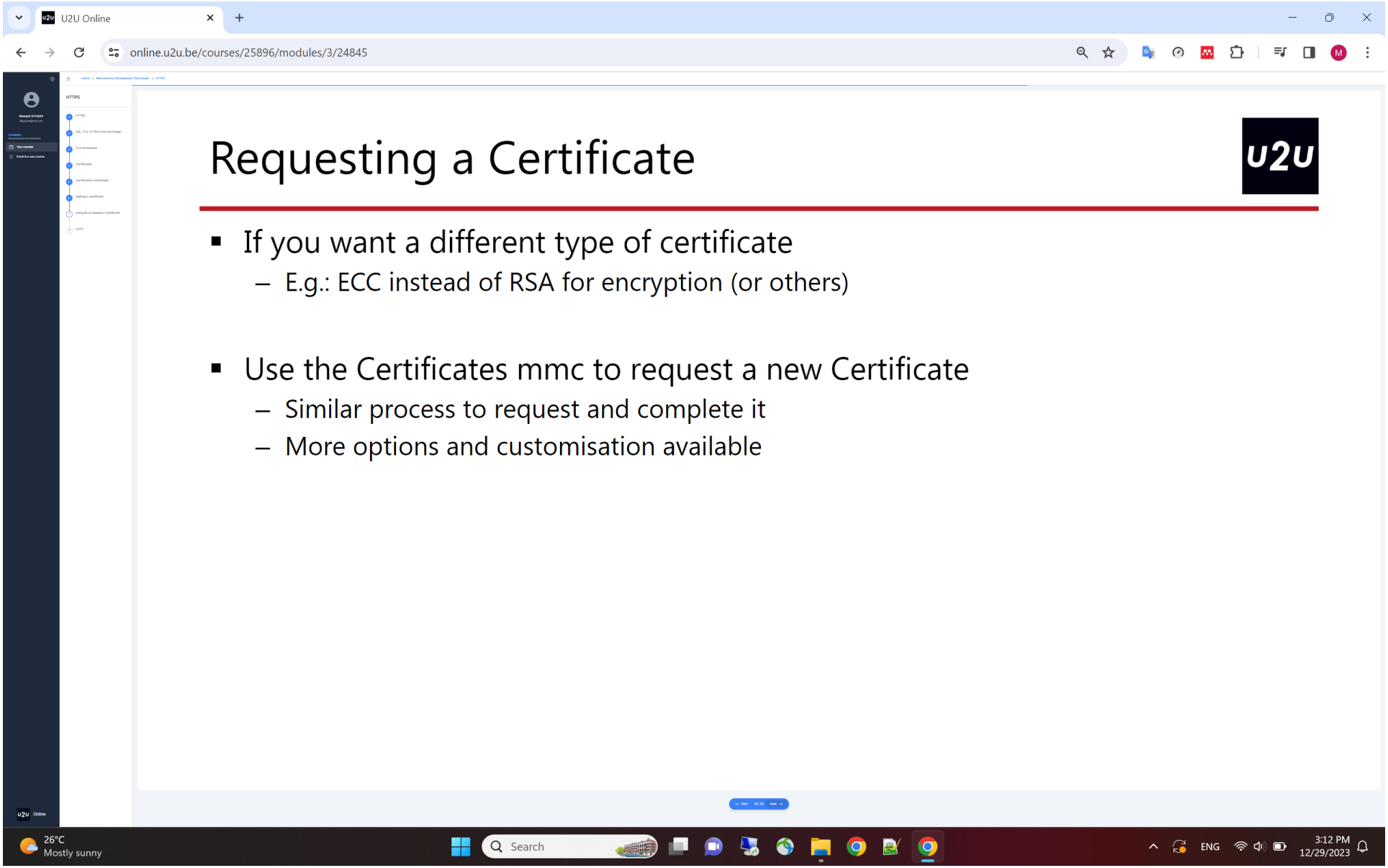

U2U Online
online.u2u.be/courses/25896/modules/3/24845
Requesting a Certificate
U2U
Name for the domain
Wildcards are available
Request Certificate
Distinguished Name Properties
Specify the required information for the certificate. State/province and City/locality must be specified as official names and they cannot contain abbreviations.
Common name: *.u2u.be
Organization: U2U Training nv
Organizational unit: IT or WHATEVER
City/locality Zellik
State/province: Vlaams-Brabant
Country/region: BE
Previous
Next
Finish
Cancel
26°C
Mostly sunny
Search
ENG
3:12 PM
12/29/2023

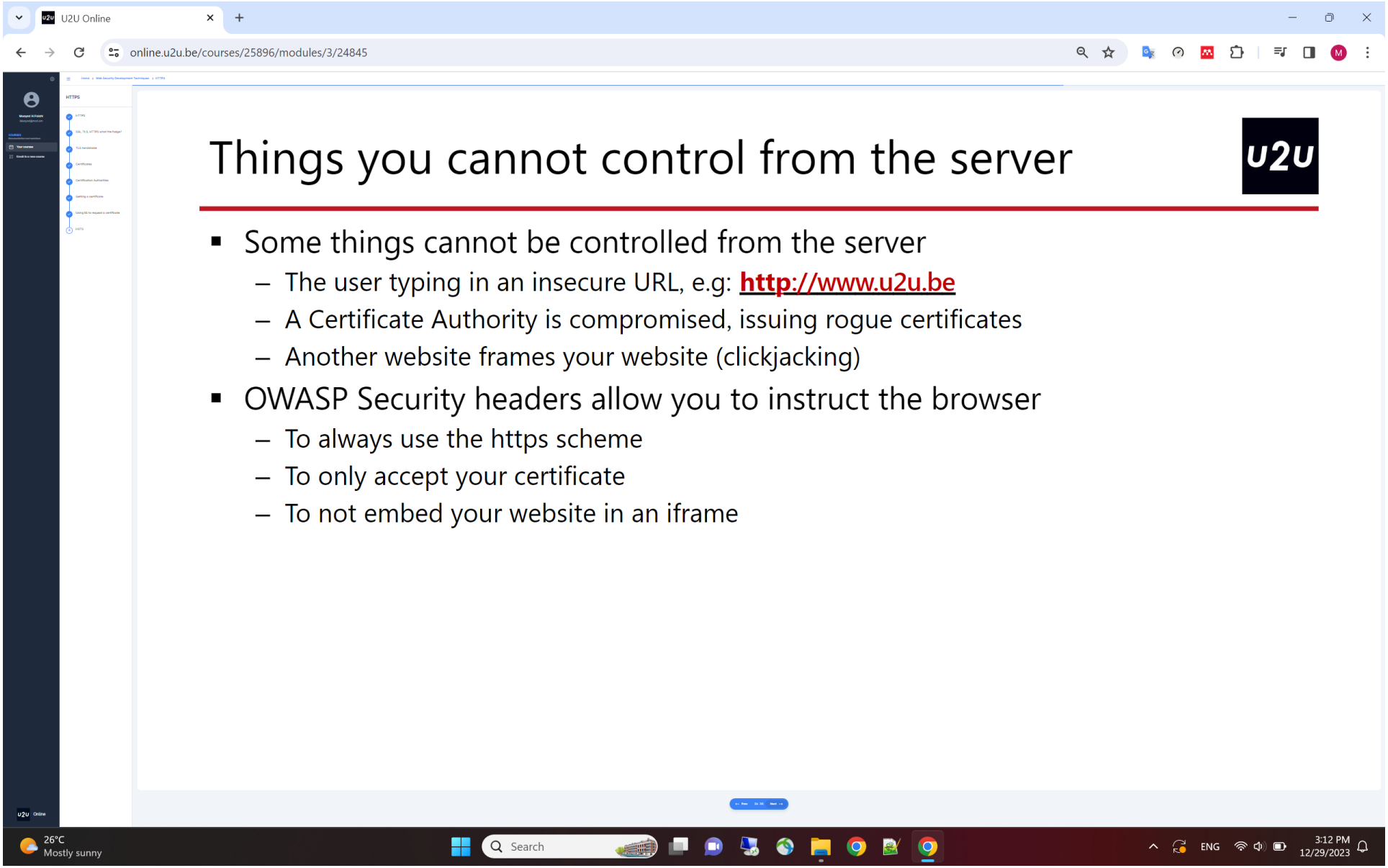

U2U Online
online.u2u.be/courses/25896/modules/3/24845
Requesting a Certificate
u2u
Request Certificate
Cryptographic Service Provider Properties
Select a cryptographic service provider and a bit length. The bit length of the encryption key determines the certificate's encryption strength. The greater the bit length, the stronger the security. However, a greater bit length may decrease performance.
Cryptographic service provider:
Microsoft RSA SChannel Cryptographic Provider
Bit length:
2048
Previous
Next
Finish
Cancel
26°C
Mostly sunny
Search
ENG
3:12 PM
12/29/2023

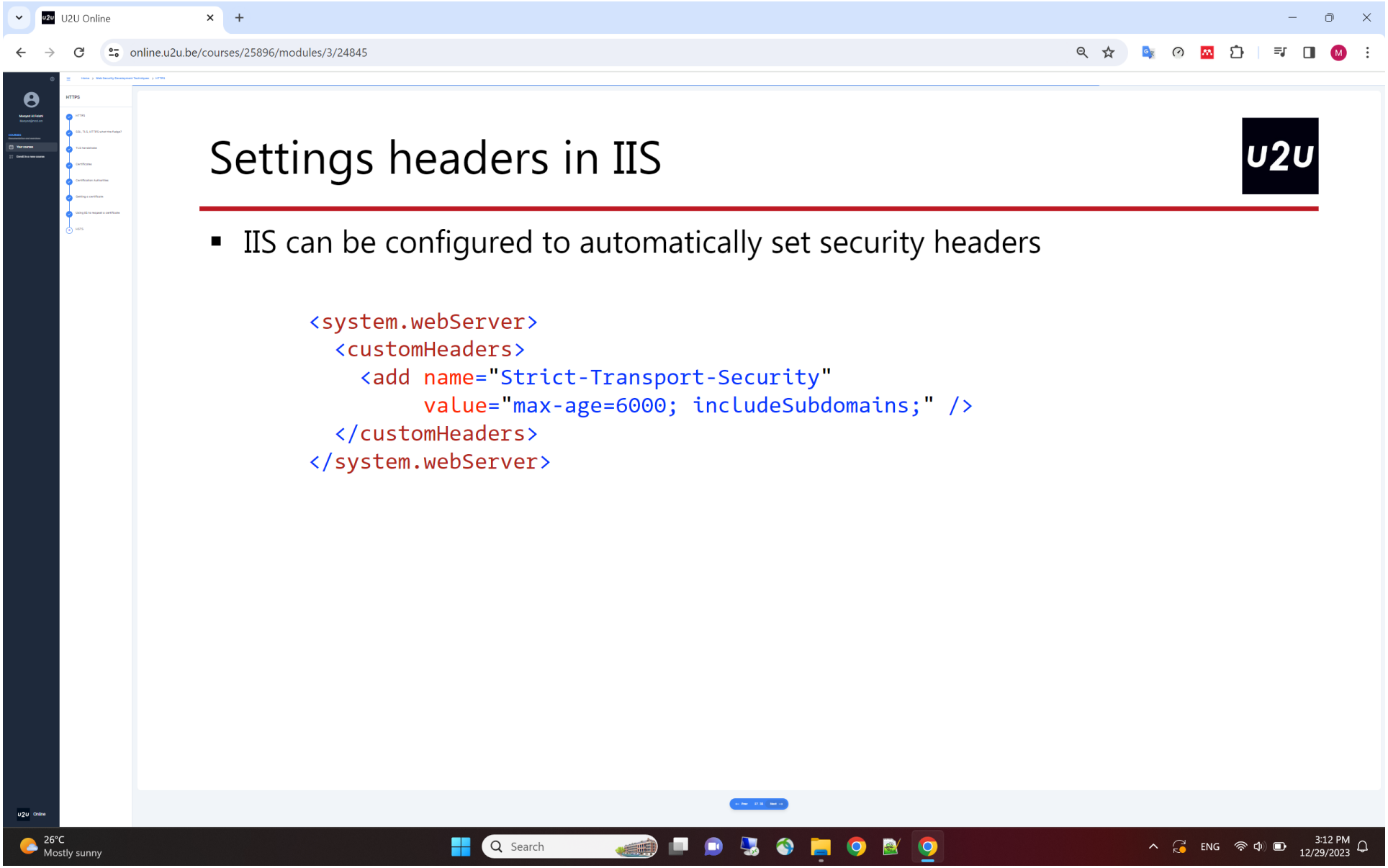
Requesting a Certificate

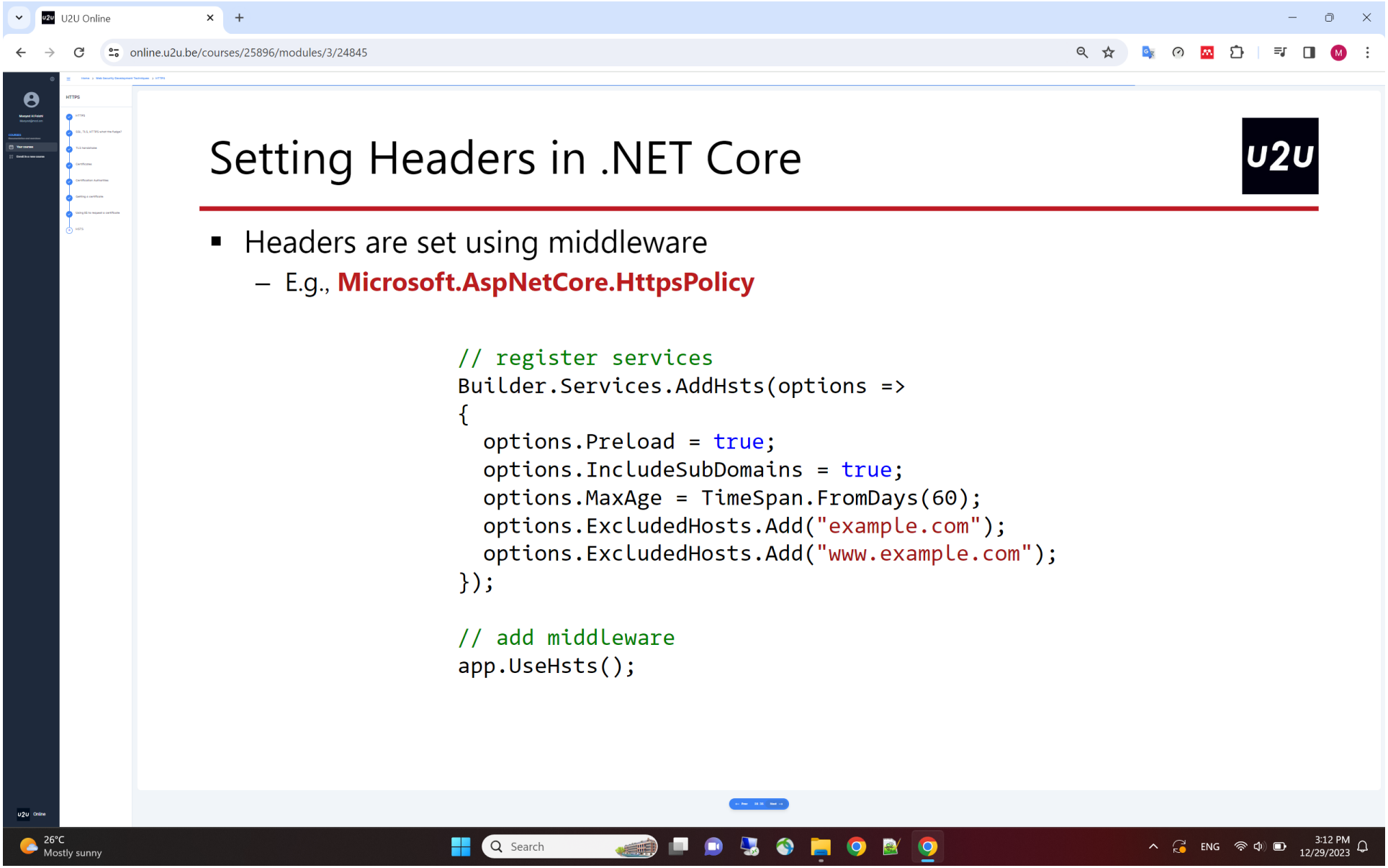
- Store the certificate request on your filesystem
- Go to a Certificate Authority
  - Symantec, Comodo Secure, RapidSSL, Let's Encrypt...
- Buy a new certificate (and supply them your request)
- Get the response back and use IIS to complete the request

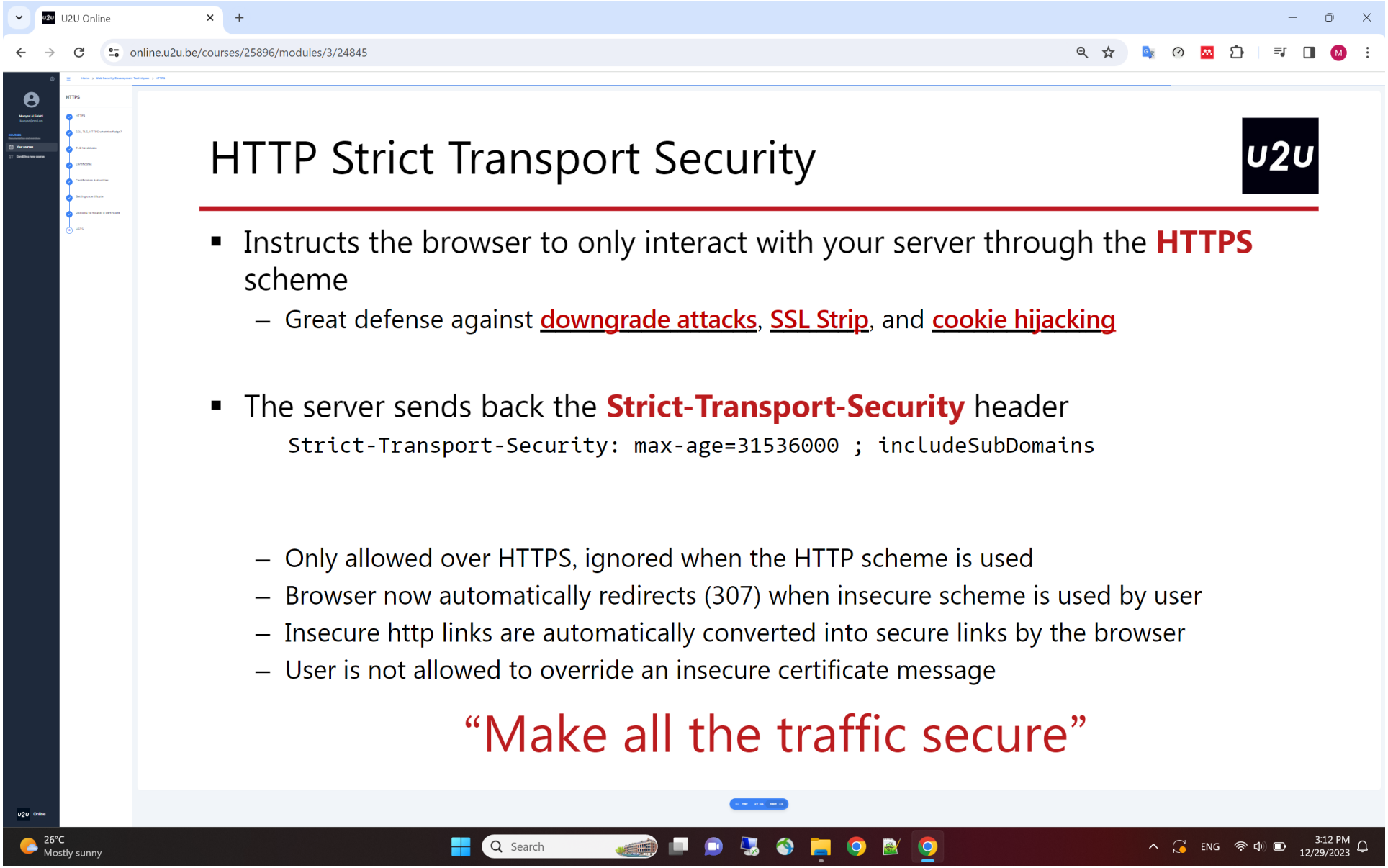


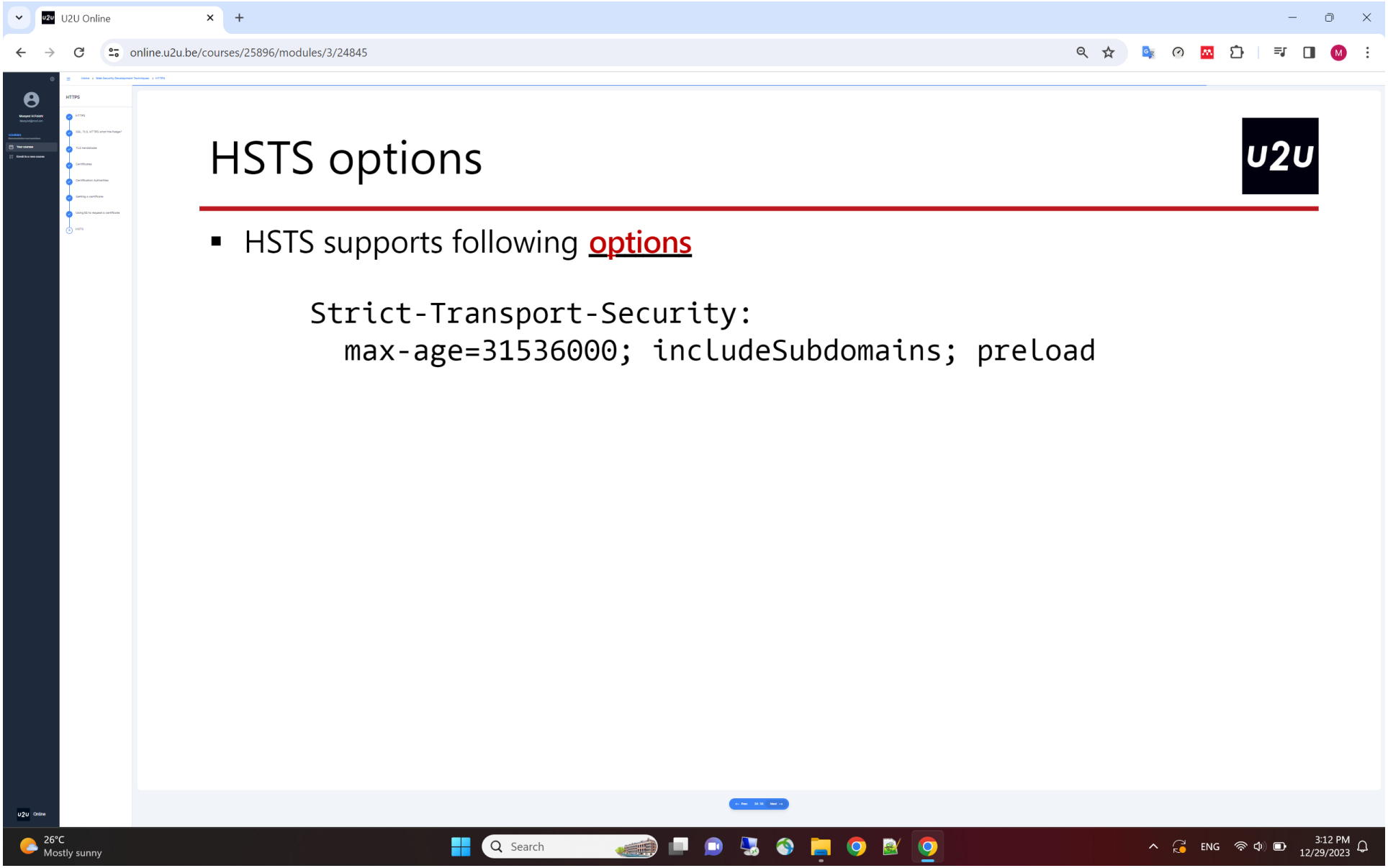

U2U Online
online.u2u.be/courses/25896/modules/3/24845
Requesting a Certificate
u2u
If you want a different type of certificate
E.g.: ECC instead of RSA for encryption (or others)
Use the Certificates mmc to request a new Certificate
Similar process to request and complete it
More options and customisation available
26°C
Mostly sunny
Search
ENG
3:12 PM
12/29/2023

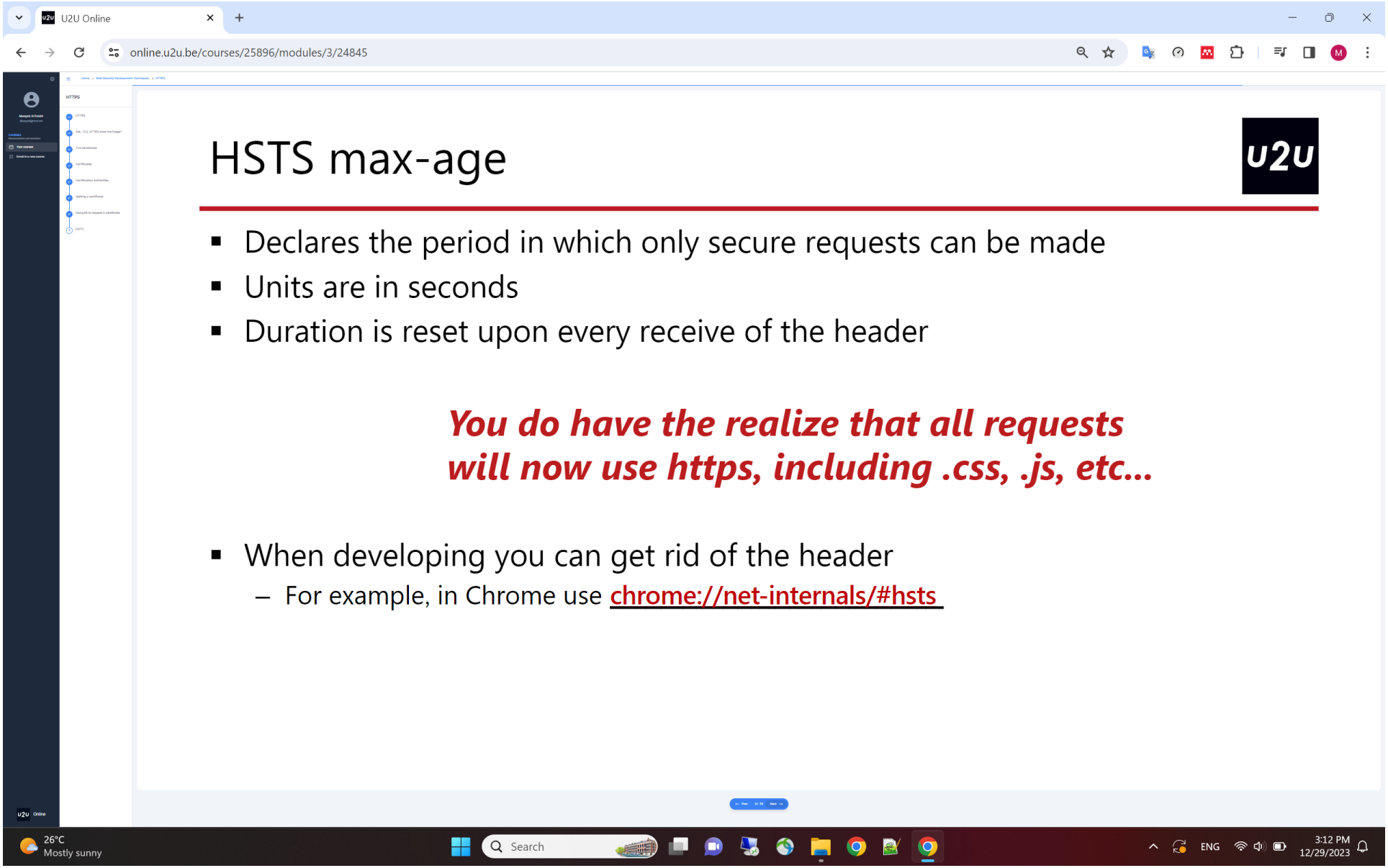

U2U Online
online.u2u.be/courses/25896/modules/3/24845
HTTPS
Things you cannot control from the server
U2U
Some things cannot be controlled from the server
The user typing in an insecure URL, e.g: http://www.u2u.be
A Certificate Authority is compromised, issuing rogue certificates
Another website frames your website (clickjacking)
OWASP Security headers allow you to instruct the browser
To always use the https scheme
To only accept your certificate
To not embed your website in an iframe
26°C
Mostly sunny
Search
ENG
3:12 PM
12/29/2023

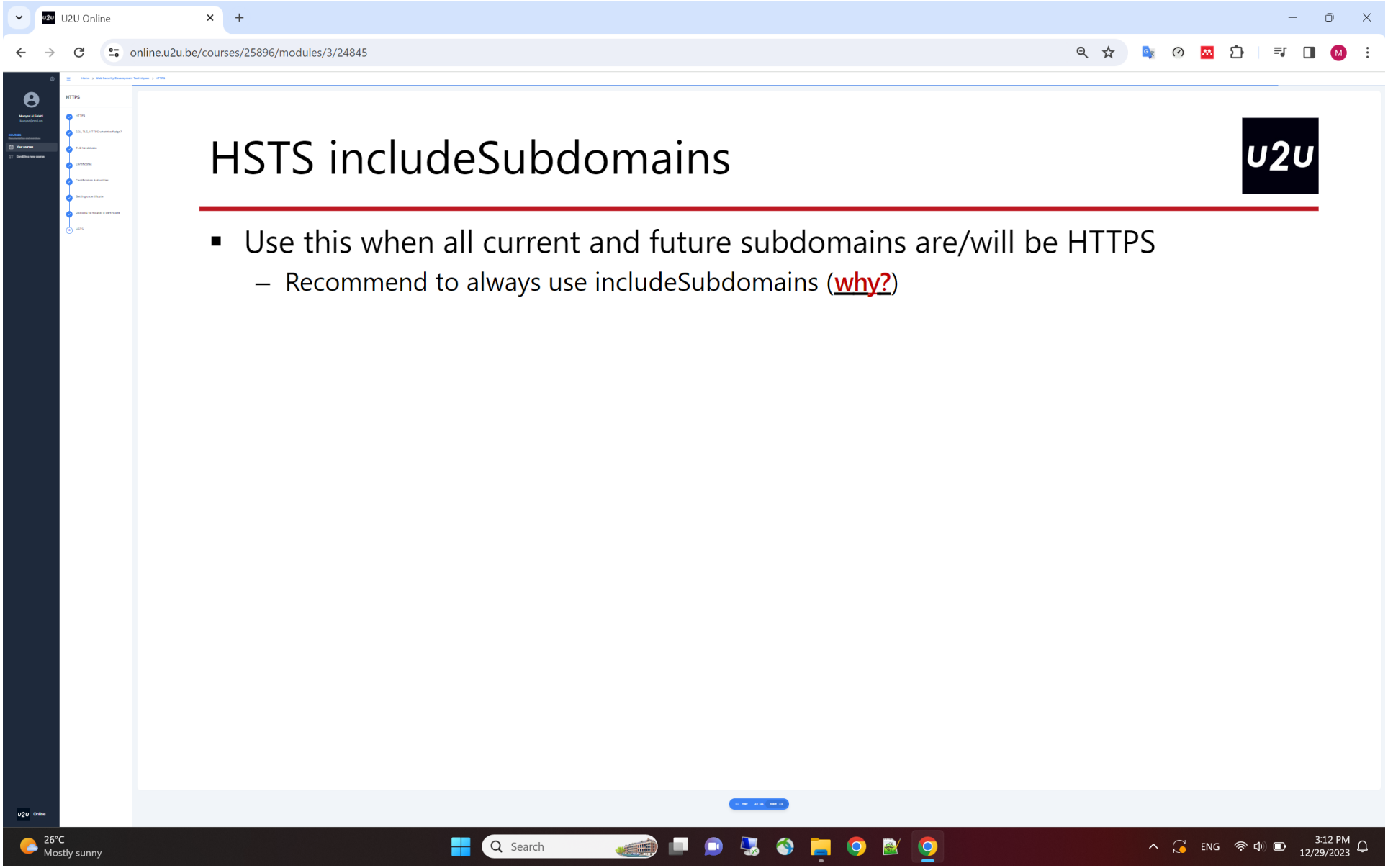

U2U Online
online.u2u.be/courses/25896/modules/3/24845
HTTPS
Settings headers in IIS
U2U
IIS can be configured to automatically set security headers
<system.webServer>
<customHeaders>
<add name="Strict-Transport-Security"
value="max-age=6000; includeSubdomains;" />
</customHeaders>
</system.webServer>
26°C
Mostly sunny
Search
ENG
3:12 PM
12/29/2023

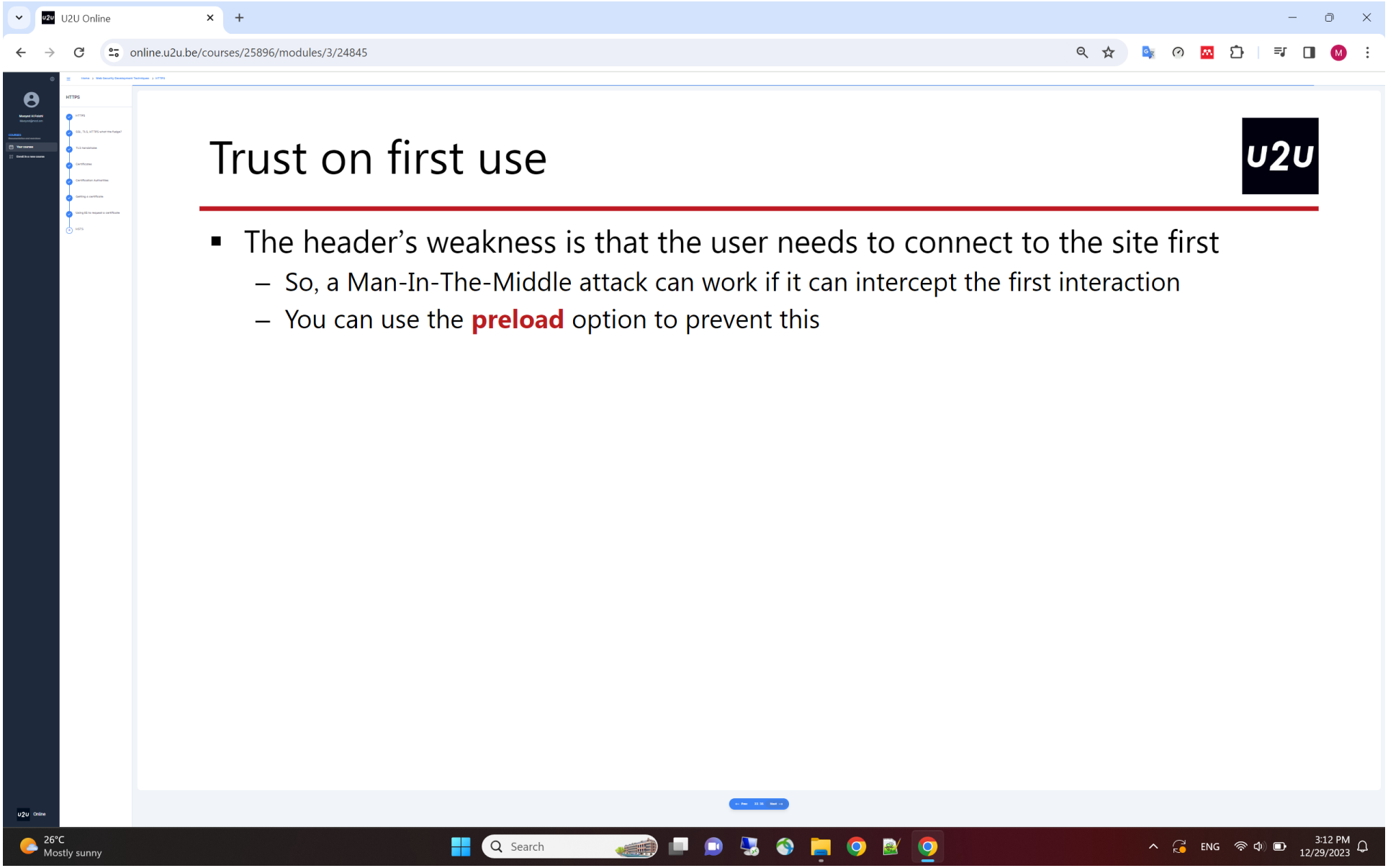

U2U Online
online.u2u.be/courses/25896/modules/3/24845
Setting Headers in .NET Core
u2u
Headers are set using middleware
E.g., Microsoft.AspNetCore.HttpsPolicy
// register services
Builder.Services.AddHsts(options =>
{
options.Preload = true;
options.IncludeSubDomains = true;
options.MaxAge = TimeSpan.FromDays(60);
options.ExcludedHosts.Add("example.com");
options.ExcludedHosts.Add("www.example.com");
});
// add middleware
app.UseHsts();
26°C
Mostly sunny
Search
ENG
3:12 PM
12/29/2023

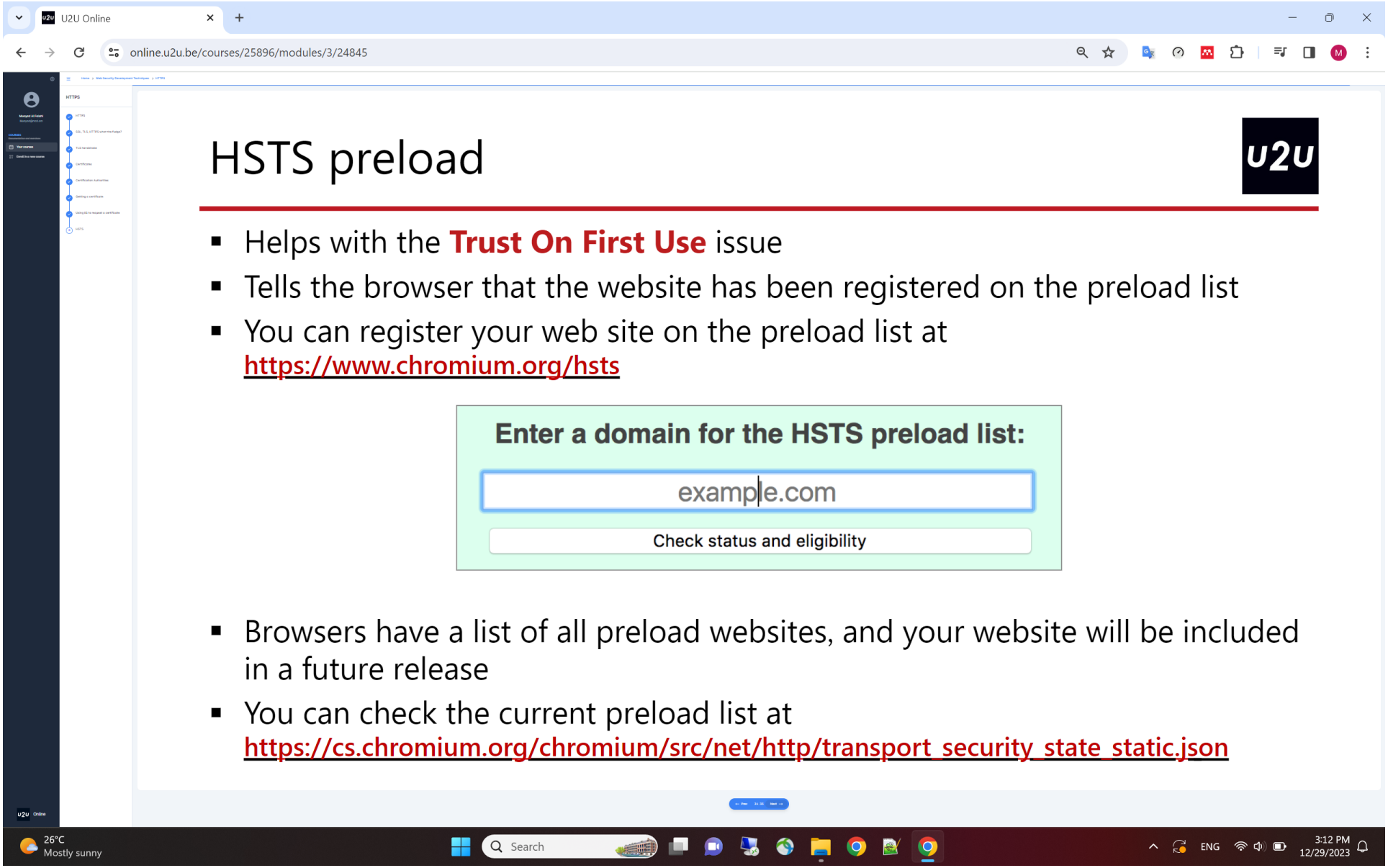

U2U Online
online.u2u.be/courses/25896/modules/3/24845
HTTPS
HTTP Strict Transport Security
u2u
Instructs the browser to only interact with your server through the HTTPS scheme
Great defense against downgrade attacks, SSL Strip, and cookie hijacking
The server sends back the Strict-Transport-Security header
Strict-Transport-Security: max-age=31536000 ; includeSubDomains
Only allowed over HTTPS, ignored when the HTTP scheme is used
Browser now automatically redirects (307) when insecure scheme is used by user
Insecure http links are automatically converted into secure links by the browser
User is not allowed to override an insecure certificate message
“Make all the traffic secure”
26°C
Mostly sunny
Search
ENG
3:12 PM
12/29/2023

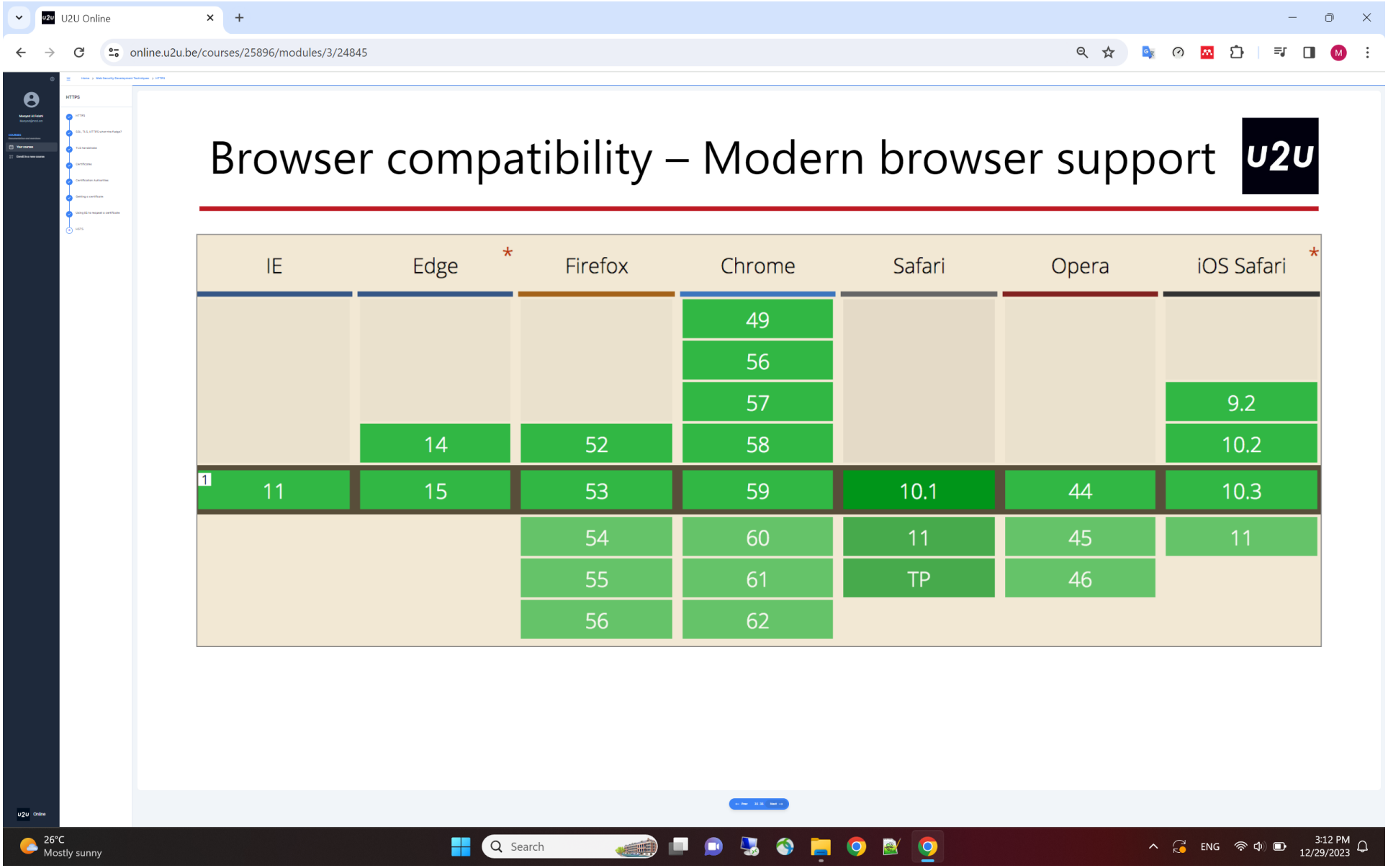

U2U Online
online.u2u.be/courses/25896/modules/3/24845
HTTPS
HSTS options
u2u
HSTS supports following options
Strict-Transport-Security:
max-age=31536000; includeSubdomains; preload
26°C
Mostly sunny
Search
ENG
3:12 PM
12/29/2023


U2U Online
online.u2u.be/courses/25896/modules/3/24845
HSTS max-age
u2u
Declares the period in which only secure requests can be made
Units are in seconds
Duration is reset upon every receive of the header
You do have the realize that all requests will now use https, including .css, .js, etc...
When developing you can get rid of the header
For example, in Chrome use chrome://net-internals/#hsts
26°C
Mostly sunny
Search
ENG
3:12 PM
12/29/2023


U2U Online
online.u2u.be/courses/25896/modules/3/24845
HTTPS
HSTS includeSubdomains
u2u
Use this when all current and future subdomains are/will be HTTPS
Recommend to always use includeSubdomains (why?)
26°C
Mostly sunny
Search
ENG
3:12 PM
12/29/2023


U2U Online
online.u2u.be/courses/25896/modules/3/24845
HTTPS
Trust on first use
U2U
The header's weakness is that the user needs to connect to the site first
So, a Man-In-The-Middle attack can work if it can intercept the first interaction
You can use the preload option to prevent this
26°C
Mostly sunny
Search
ENG
3:12 PM
12/29/2023


U2U Online
online.u2u.be/courses/25896/modules/3/24845
HTTPS
HSTS preload
U2U
Helps with the Trust On First Use issue
Tells the browser that the website has been registered on the preload list
You can register your web site on the preload list at https://www.chromium.org/hsts
Enter a domain for the HSTS preload list:
example.com
Check status and eligibility
Browsers have a list of all preload websites, and your website will be included in a future release
You can check the current preload list at https://cs.chromium.org/chromium/src/net/http/transport_security_state_static.json
26°C
Mostly sunny
Search
ENG
3:12 PM
12/29/2023


U2U Online
online.u2u.be/courses/25896/modules/3/24845
Browser compatibility – Modern browser support
u2u
IE
Edge *
Firefox
Chrome
Safari
Opera
iOS Safari *
49
56
57
9.2
14
52
58
10.2
1
11
15
53
59
10.1
44
10.3
54
60
11
45
11
55
61
TP
46
56
62
26°C
Mostly sunny
Search
ENG
3:12 PM
12/29/2023