

u2u U2U Online

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

Home > Web Security Fundamentals > HTTPS

HTTPS

u2u

Developer and IT Training

SSL, TLS, HTTPS: what the fudge?

TLS handshake

Certificates

Certification authorities

Getting a certificate

Using ED to request a certificate

HTTP

26°C Mostly sunny

Search

3:11 PM 12/29/2023

This screenshot shows a web browser window displaying a course page from 'u2u Online'. The main content area features a large red header with the text 'Developer and IT Training' and a 'u2u' logo. Below this, the word 'HTTPS' is prominently displayed. To the left of the main content, there is a sidebar with a navigation menu for 'HTTPS' topics. The browser's address bar shows the URL 'online.u2u.be/courses/25896/modules/3/24845'. The taskbar at the bottom of the screen includes icons for the Start button, search, file explorer, and various system status indicators like battery level and network connection.

The screenshot shows a web browser window titled "U2U Online" with the URL "online.u2u.be/courses/25896/modules/3/24845". The page content is a presentation slide with the following structure:

- Agenda**
- SSL, TLS, HTTPS – what the fudge?
- TLS Handshake
- Certificates
- Certification Authorities
- Getting a Certificate
- HSTS

The browser interface includes a sidebar with user information ("Maged AlFayez MagedAlFayez"), a navigation menu ("Your courses", "Send this course"), and a toolbar with various icons. The system tray at the bottom shows weather (26°C, Mostly sunny), a search bar, and system status indicators.

SSL, TLS, HTTPS,... What the fudge?

- **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 3:11 PM 12/29/2023

The screenshot shows a web browser window with the URL [online.u2u.be/courses/25896/modules/3/24845](https://online.u2u.be/courses/25896/modules/3/24845). The page title is "History of SSL". On the left, there's a sidebar with a navigation tree under "HTTPS" and a user profile on the right with the "u2u" logo.

# History of SSL

---

- 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

At the bottom, the taskbar shows the weather (26°C, Mostly sunny), a search bar, and various application icons (File Explorer, Task View, Edge, File History, Google Chrome). The system tray shows the date (12/29/2023) and time (3:11 PM).

The screenshot shows a web browser window with the following details:

- Title Bar:** U2U Online
- Address Bar:** online.u2u.be/courses/25896/modules/3/24845
- Page Content:**
  - Section Header:** History of TLS
  - Text:** TLS: to open-source the protocol, it was renamed from SSL
  - List:**
    - 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
  - Link:** [https://en.wikipedia.org/wiki/Transport\\_Layer\\_Security#TLS\\_1.3](https://en.wikipedia.org/wiki/Transport_Layer_Security#TLS_1.3)

**Bottom Taskbar:**

  - 26°C Mostly sunny
  - Search bar
  - Icons for File Explorer, Task View, Control Panel, Internet Explorer, Google Chrome, and File Explorer
  - System icons: battery, signal, volume, language (ENG), and date (12/29/2023)

u2u U2U Online

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

# Protection with HTTPS

- 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

3:11 PM 12/29/2023

**u2u U2U Online**

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

Home > Web Security Handshake Techniques > HTTPS

HTTPS

- HTTPS
- SSL, TLS, HTTPS what the fudge?
- TLS handshake
  - Certificates
  - Certification authorities
  - Getting a certificate
  - Using RSA to request a certificate
- HTTP

# 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

3:11 PM 12/29/2023

HTTP over TLS handshake

```

    graph LR
        subgraph Browser [Browser]
            direction TB
            B1[1. ClientHello] --> S2[2. ServerHello]
            S3[3. Server Certificate] --> C4[4. Client Key Exchange]
            C4 --> S5[5. Decrypt]
            S5 --> E6[6. Encrypt & Decrypt using shared secret]
            E6 --> T7[TXT]
        end
        subgraph Server [Server]
            direction TB
            P1[Public key] --> S2
            S2 --> S3
            S3 --> P2[Private key]
            P2 --> S5
            S5 --> E6
            E6 --> T7
        end
        T7 --> C4
    
```

The diagram illustrates the TLS handshake process between a Browser and a Server. The process consists of six main steps:

- 1. ClientHello**: Sent from the Browser to the Server.
- 2. ServerHello**: Sent from the Server to the Browser, indicating the chosen cipher suite and sending its public key.
- 3. Server Certificate**: Sent from the Server to the Browser, containing the server's certificate.
- 4. Client Key Exchange**: Sent from the Browser to the Server, containing the shared master key.
- 5. Decrypt**: The Server uses its private key to decrypt the message sent in step 4.
- 6. Encrypt & Decrypt using shared secret**: Both parties use the shared master key to encrypt and decrypt messages.

After the handshake, the data is transmitted in **Cipher text** format between the two parties, which are then decrypted back into **TXT** (Text) format.

The screenshot shows a web browser window with the URL [online.u2u.be/courses/25896/modules/3/24845](https://online.u2u.be/courses/25896/modules/3/24845). The page title is "Certificates". On the left, there is a sidebar with a navigation tree under "HTTPS": "HTTP", "TLS handshake", "Certificates", "Certification authorities", "Getting a certificate", and "Using ED to request a certificate". The main content area contains the following text:

- 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

The browser interface includes a search bar, a toolbar with various icons, and a system tray at the bottom showing weather (26°C, Mostly sunny), date (12/29/2023), and time (3:11 PM).

The screenshot shows a web browser window with the following details:

- Title Bar:** U2U Online
- Address Bar:** online.u2u.be/courses/25896/modules/3/24845
- Page Content:**
  - Section Title:** Authenticity, Integrity and Privacy
  - List:**
    - 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...
- Left Sidebar:** A navigation tree for "HTTPS" topics, including "What is HTTPS?", "TLS handshake", "Certificates", "Certificate authorities", "Getting a certificate", and "Using TLS to request a certificate".
- Right Sidebar:** The "u2u" logo.
- Bottom Taskbar:** Shows the Windows Start button, a search bar, pinned icons for File Explorer, Google Chrome, and others, and system status icons for battery, signal, and date/time (3:11 PM, 12/29/2023).

u2u U2U Online

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

Home > Web Security Fundamentals > HTTPS

HTTPS

- HTTP
- TLS / SSL, HTTPS when the https!
- TLS handshake
- Certificates
- Certificate authorities
- Getting a certificate
- Using ED to request a certificate
- HTTPS

# Certificate Authorities

u2u

- 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



Root CA

CA CA

User User User

26°C Mostly sunny

Search

3:11 PM 12/29/2023

The screenshot shows a web browser window with the URL [online.u2u.be/courses/25896/modules/3/24845](https://online.u2u.be/courses/25896/modules/3/24845). The slide title is "Trust Chain". On the left, there's a sidebar with navigation links like "My profile", "Your courses", and "Getting started". The main content area contains a bulleted list about certificate validation and trust chains.

## Trust Chain

- 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**

U2U Online

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

# Certificate Checks

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

26°C  
Mostly sunny

Search

3:11 PM 12/29/2023

u2u U2U Online

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

# Identity Confirmation

- 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

- HTTPS
- SSL, TLS, HTTPS what the fudge?
- TLS handshake
- Certificates
- Certification authorities
- Getting a certificate
- Using ED to request a certificate
- HTTPS

u2u

https://www.amazon.nl/

GitHub, Inc. [US] https://github.com/

26°C Mostly sunny

Search

3:11 PM 12/29/2023

The screenshot shows a web browser window with the following details:

- Title Bar:** U2U Online
- Address Bar:** online.u2u.be/courses/25896/modules/3/24845
- Page Content:**
  - Section Title:** Expiration and Revocation
  - List:**
    - 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**
- Left Sidebar:** A navigation tree for the 'HTTPS' module, including 'Introduction', 'TLS handshake', 'Certificates', 'Certification authorities', 'Getting a certificate', 'Using RSA to request a certificate', and 'HTTP'.
- Right Sidebar:** The 'u2u' logo.
- Bottom Taskbar:** Shows the Windows Start button, a search bar, pinned icons for File Explorer, Task View, Edge, Google Chrome, and File History, and system status icons for battery, signal, volume, and date/time (3:11 PM, 12/29/2023).

The screenshot shows a Microsoft Edge browser window with the following details:

- Title Bar:** U2U Online
- Address Bar:** online.u2u.be/courses/25896/modules/3/24845
- Page Content:**
  - Section Header:** Digital Certificate
  - List:**
    - 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 in a secure place!
      - The Certification Authority checks everything and sends you a signed certificate
  - Footer:** A red link: <https://blogs.u2u.be/peter/post/configure-https-with-letsencrypt-manually>

The browser interface includes a sidebar with user information, a navigation menu, and a bottom taskbar with various icons.

u2u U2U Online

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

Home > Web Security Intermediate Techniques > 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:
            56:74:28:01:9c: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:ea:08:6d: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...+....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

3:11 PM 12/29/2023

U2U Online

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

# Digital Certificate

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

**Certificate Information**

This certificate is intended for the following purpose(s):

- Ensures the identity of a remote computer
- Proves your identity to a remote computer

\* Refer to the certification authority's statement for details.

**Issued to:** www.u2u.be

**Issued by:** RapidSSL SHA256 CA - G3

**Valid from** 14/05/2015 **to** 16/05/2017

Issuer Statement

OK

26°C Mostly sunny

Search

3:11 PM 12/29/2023

The screenshot shows a web browser window with the URL [online.u2u.be/courses/25896/modules/3/24845](https://online.u2u.be/courses/25896/modules/3/24845). The page title is "Types of Certificates". On the left, there is a sidebar with a navigation tree under "HTTPS" and a user profile section. On the right, there is a large "u2u" logo. The main content area contains a bulleted list of certificate types:

- 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

The bottom of the screen shows a taskbar with various icons and system status information.

u2u U2U Online

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

HTTPS

- HTTP
- SSL, TLS, HTTPS wrap the hedge!
- TLS handshake
- Certificates
- Certificate authorities
- Getting a certificate
- Using IIS to request a certificate
- HTTPS

# Requesting a Certificate

u2u

Internet Information Services (IIS) Manager

File View Help

Connections WIN- [WIN-DP]

WIN- Home

Filter: Go Show All Group by: Area

ASP.NET

- .NET Authorization
- .NET Compilation
- .NET Error Pages
- .NET Globalization
- .NET Trust Levels
- Application Settings
- Connection Strings
- Machine Key
- Pages and Controls
- Providers
- Session State
- SMTP E-mail

IIS

- Authentication
- Compression
- Default Document
- Directory Browsing
- Error Pages
- Handler Mappings
- HTTP Redirect
- HTTP Response
- ISAPI and CGI Restrictions
- ISAPI Filters
- Logging
- MIME Types
- Modules
- Output Caching

Management

- Request Filtering
- Server Certificates
- WebDAV Authorization
- Worker Processes

Actions

- Manage Server
- Restart
- Start
- Stop
- View Application Pools
- View Sites
- Change .NET Framework Version
- Get New Web Platform Components
- Help

26°C Mostly sunny

Search

3:12 PM 12/29/2023

A large red arrow points from the 'Server Certificates' icon in the IIS Manager interface below to the 'Getting a certificate' step in the guide above.

The screenshot shows a web browser window with the URL [online.u2u.be/courses/25896/modules/3/24845](https://online.u2u.be/courses/25896/modules/3/24845). The page title is "Requesting a Certificate". On the left, there's a sidebar with a navigation tree under "HTTPS" and a "Your courses" section. The main content area displays a "Server Certificates" table with several entries. To the right of the table is an "Actions" sidebar with various options. A large red arrow points to the "Create Certificate Request..." button in this sidebar.

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	[REDACTED]	[REDACTED]	22/05/2026 12:28:21	67000F9CEC790D7A5AE3812...	Personal
WMSVC-SHA2	[REDACTED]	[REDACTED]	23/07/2026 14:58:29	F6C0BF56075003484FD465A53...	Personal
WMSVC-SHA2	[REDACTED]	[REDACTED]	28/06/2026 3:28:52	DA77E5B999124D269F7A27FD...	Personal
WMSVC-SHA2	[REDACTED]	[REDACTED]	24/06/2026 9:50:56	AF65F621FB91CF72A555349B...	Personal
WMSVC-SHA2	[REDACTED]	[REDACTED]	15/07/2026 20:16:06	470256584CD5DD6037F358DB...	Personal

u2u U2U Online

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

HTTPS

Request Certificate

Distinguished Name Properties

Name for the domain  
Wildcards are available

Common name: \*.u2u.be

Organization: U2U Training nv

Organizational unit: IT or WHATEVER

City/locality: Zellik

State/province: Vlaams-Brabant

Country/region: BE

Next

26°C Mostly sunny

Search

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

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

Complete Certificate Request

Specify Certificate Authority Response

Complete a previously created certificate request by retrieving the file that contains the certificate authority's response.

File name containing the certification authority's response:

Friendly name:

Select a certificate store for the new certificate:

Personal

The screenshot shows a web browser window with the URL [online.u2u.be/courses/25896/modules/3/24845](https://online.u2u.be/courses/25896/modules/3/24845). The page title is "Requesting a Certificate". On the left, there is a sidebar with a navigation tree under "HTTPS" and a "Your notes" section. The main content area contains two bullet points:

- 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

The browser interface includes a search bar, a toolbar with various icons, and a system tray at the bottom showing weather, battery, and system status.

# Things you cannot control from the server

- 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

Settings headers in IIS

- 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>
```

The screenshot shows a web browser window with the URL [online.u2u.be/courses/25896/modules/3/24845](https://online.u2u.be/courses/25896/modules/3/24845). The page title is "Setting Headers in .NET Core". On the left, there's a sidebar with a navigation tree under "HTTPS" and a "Your notes" section. On the right, the main content area displays a slide with a red header and a "u2u" logo. The slide content includes a bulleted list and a code snippet.

- 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();
```

# HTTP Strict Transport Security

- 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”**

The screenshot shows a Microsoft Edge browser window. The address bar displays `online.u2u.be/courses/25896/modules/3/24845`. The main content area is titled "HSTS options". On the left, there's a sidebar with a navigation tree under "HTTPS" and a "Your notes" section. A large "u2u" logo is in the top right corner. The bottom of the screen shows the Windows taskbar with icons for Start, Search, File Explorer, Task View, and Google Chrome, along with system status icons like battery level, signal strength, and volume.

# HSTS options

- HSTS supports following options

Strict-Transport-Security:  
max-age=31536000; includeSubdomains; preload

The screenshot shows a web browser window with the URL [online.u2u.be/courses/25896/modules/3/24845](https://online.u2u.be/courses/25896/modules/3/24845). The slide title is "HSTS max-age". On the left, there's a sidebar with a navigation tree under "HTTPS" and a "u2u" logo. The main content area contains a bulleted list and a red text quote. At the bottom, there's a taskbar with weather, search, and system icons.

## HSTS max-age

- 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>

The screenshot shows a web browser window with the following details:

- Title Bar:** U2U Online
- Address Bar:** online.u2u.be/courses/25896/modules/3/24845
- Page Content:**
  - Section Header:** HSTS includeSubdomains
  - List:**
    - Use this when all current and future subdomains are/will be HTTPS
      - Recommend to always use includeSubdomains ([why?](#))
- Left Sidebar:** A navigation menu for "Myself & Project" with sections like "Your courses", "Certificates", and "Getting a certificate".
- Right Sidebar:** A large "u2u" logo.
- Taskbar:** Shows the Windows Start button, a search bar, pinned icons for File Explorer, Task View, Edge, and Google Chrome, and system status icons for weather (26°C, Mostly sunny), battery (3:12 PM), and connectivity.

The screenshot shows a web browser window with the following details:

- Title Bar:** U2U Online
- Address Bar:** online.u2u.be/courses/25896/modules/3/24845
- Page Content:**
  - Section Title:** Trust on first use
  - List:**
    - 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
- Left Sidebar:** Shows a navigation tree for "HTTPS" topics, including "What is HTTPS?", "TLS handshake", "Certificates", "Certification authorities", "Getting a certificate", "Using HSTS to request a certificate", and "HSTS".
- Right Sidebar:** The "u2u" logo.
- Bottom Taskbar:** Shows the Windows Start button, a search bar, pinned icons for File Explorer, Task View, Edge, Google Chrome, and others, and system status icons for battery, signal, volume, and date/time (3:12 PM, 12/29/2023).

# HSTS preload

- 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:

[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](https://cs.chromium.org/chromium/src/net/http/transport_security_state_static.json)

u2u U2U Online

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

Home > Web Security Fundamentals Techniques > HTTPS

HTTPS

- 1 HTTPS
- 2 SSL/TLS, HTTPS what the fudge?
- 3 TLS handshake
- 4 Certificates
- 5 Certification authorities
- 6 Getting a certificate
- 7 Using TLS to request a certificate
- 8 HTTPS

# Browser compatibility – Modern browser support **u2u**

IE	Edge	Firefox *	Chrome	Safari	Opera	iOS Safari *
			49			
			56			
			57			
	14	52	58			
11	15	53	59	10.1	44	9.2
		54	60	11	45	10.2
		55	61	TP	46	10.3
		56	62			11

26°C Mostly sunny

Search

3:12 PM 12/29/2023