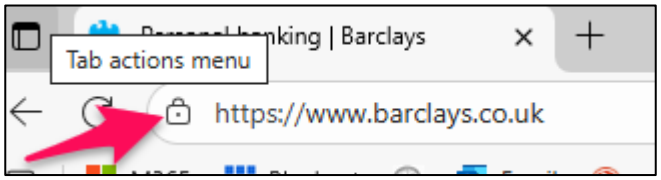
Viewing the Public Key in a Certificate During HTTPS Session Establishment

The following notes illustrate how to view the public key of barclays.co.uk - it's as good as any for example purposes. This public key is used to encrypt everything that's transmitted over the internet, from a tablet / computer onwards to barclays destination servers. The example shown here uses Microsoft Edge browser on Windows 11, however, the sequence of operations will be similar for any browser of choice.

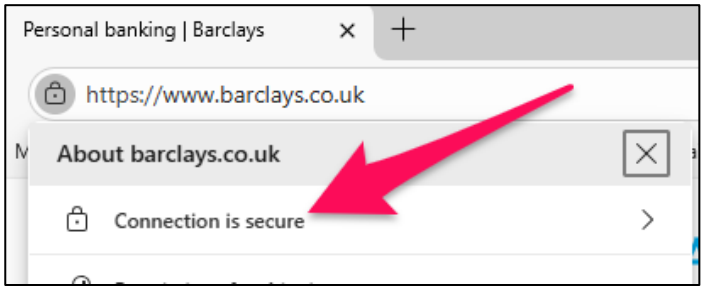
1. Access www.barclays.co.uk in a Web Browser

- Click on the padlock - to the left of https



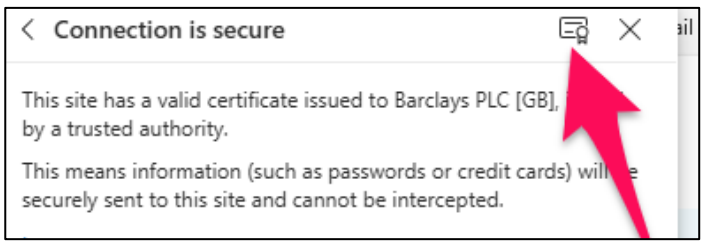
2. Security Information is Presented

- Click on the Connection is secure link (there should be similar wording in any web browser)



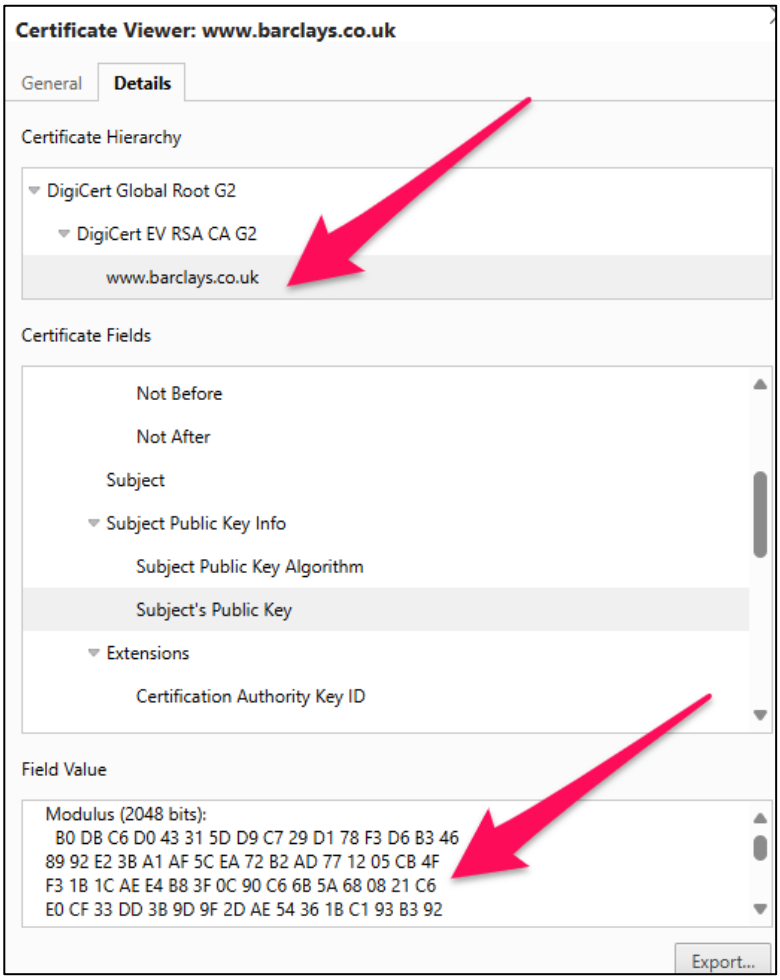
3. Confirmation that a Valid Certificate is Present

- Click on the icon representing a certificate



4. Certificate Viewer

- The subject name of the certificate (www.barclays.co.uk) and its public key can be seen. The public key is just a binary number, albeit 2048 bits long in this case - the hexadecimal value shown just makes it easier on the eyes.
- Browsers retrieve the public key (the digital binary value) to store in their cryptography caches for pending encryption purposes.
- Clicking on the export button, will commence certificate downloading (which incorporates the public key) as a file onto a local file system; it'll probably be only 3kb or 4kb in size.



Observations...

Very Public Keys

An important outcome to grasp from this technical note is that the term 'public key' is perfectly apt. Everyone on the planet with a session connected to barclays.co.uk will use the same public key to encrypt information prior to transmission.

Very Private Keys

While public keys are accessible to all, corresponding private keys are the exact opposite. These are 2,048 bit digital binary values - just like the public key. However, security around accessing private keys (key management) is the most highly restricted capability in the entire realm of IT security.