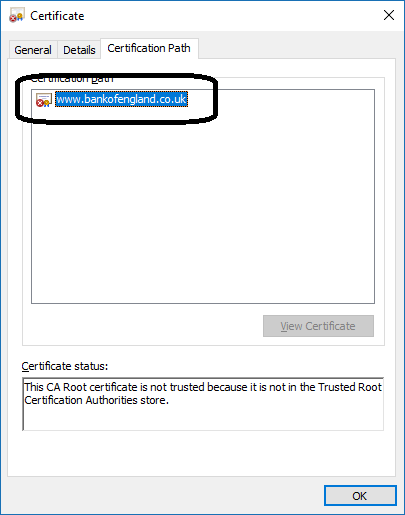
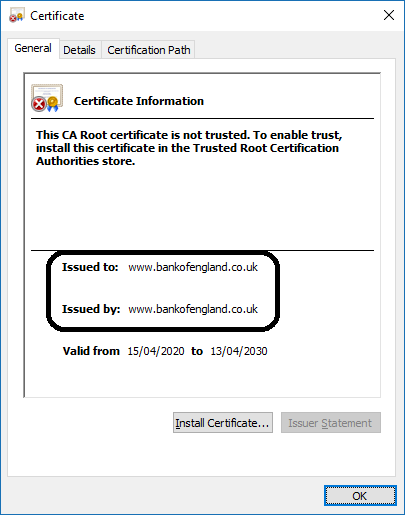
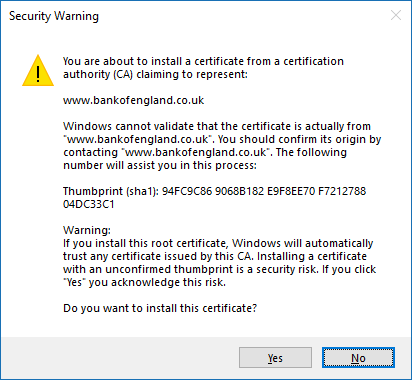
I copied detailes given in the problem and created a .cer file to have a look. As soon as I tried to install I got a thumbprint error. I believe this is a fradulent certificate file because of following reasons.

The most likely reasons are followning

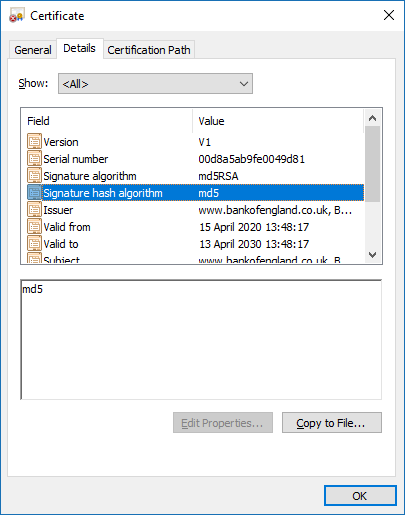


1 ) There is no certificate path e.g Server-cert – any intermediate certificate – Root Cert. While this is possible in case of a Root CA issuing a certificate to itself but from name this appears to be a certificate for external facing purpose and for that I would expect it to be signed by a trusted public certificating issuing authority like digicert and verisign. Please proceed to read further points.





2) This screenshot above confirms point 1 and when I tried to install the certificate as a Trusted root CA cert instead of an endpoint cert. I get the error above you are trying to install a certificate claiming to be www.bankofengland.co.uk



3) Using md5 as signature algorithm is not a good idea as it is old and not considered to be very secure. And can be easily forged.

<https://lwn.net/Articles/314997/>

The research combined a weakness in the certificate generation process with the ability to create MD5 hash collisions and generated a certificate that would be accepted by all browsers. That certificate could be used to sign other certificates, allowing the researchers to create a valid certificate purporting to be from any domain they chose.

Eventually, MD5 will no longer be accepted as the hash used in the signatures on certificates—or anything else, probably—but as of now, SSL implementations will accept them. There are large numbers of such certificates in use today, so browsers cannot just stop accepting them. CAs are generally offering their customers free replacement certificates that use SHA-1. Because users rarely root through the certificates presented to their browser to determine what hash algorithm was used, there is a [extension for Firefox called SSL Blacklist](http://codefromthe70s.org/sslblacklist.aspx) that detects these certificates and pops up a warning.