


National University of Computer and Emerging Sciences, Lahore Campus

	Course Name:	Information Security	Course Code:	CS3002
	Program:	BS-CS	Semester:	Fall 2024
	Section	C, D, E	Total Marks:	10
	Due Date:	06-10-2024	Weight	~3.3%
	Exam Type:	Assignment 2	Page(s):	2

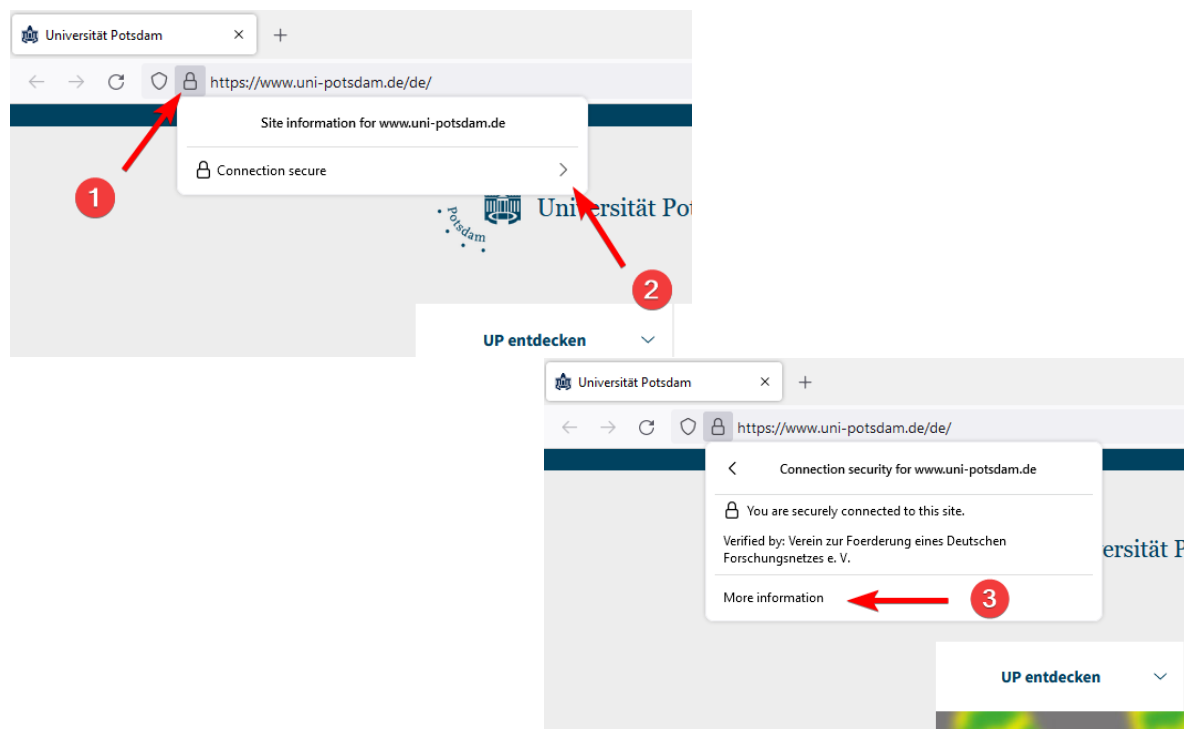
Background

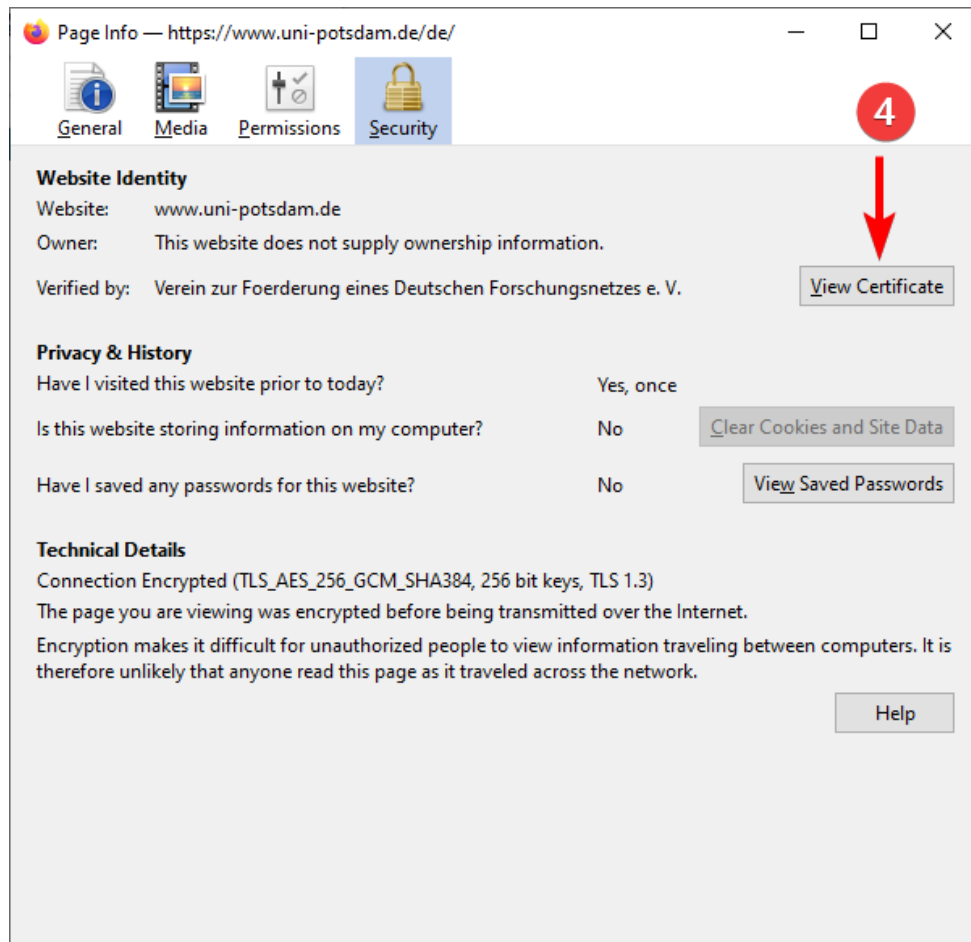
Digital Certificates are used to provide a verification of public keys. All certificates have an expiry date, but the certificate authorities may sometimes revoke a certificate before its expiry. It could be on the request of the subject (to whom certificate was issued), or upon discovery of improper certificate issuance procedures.

Therefore, when a client such as a web browser inspects a certificate, they also need to ensure it has not been revoked by the CA. One of the methods to check revocation status is the Online Certificate Status Protocol (OCSP). CAs should maintain their OCSP servers that respond to client's certificate status queries.

Practical Tasks

Choose a relatively unknown HTTPS website (so that each student picks a different one). Visit this website in **Firefox** browser. Click the lock icon in address bar and follow the steps below to open the site certificate.

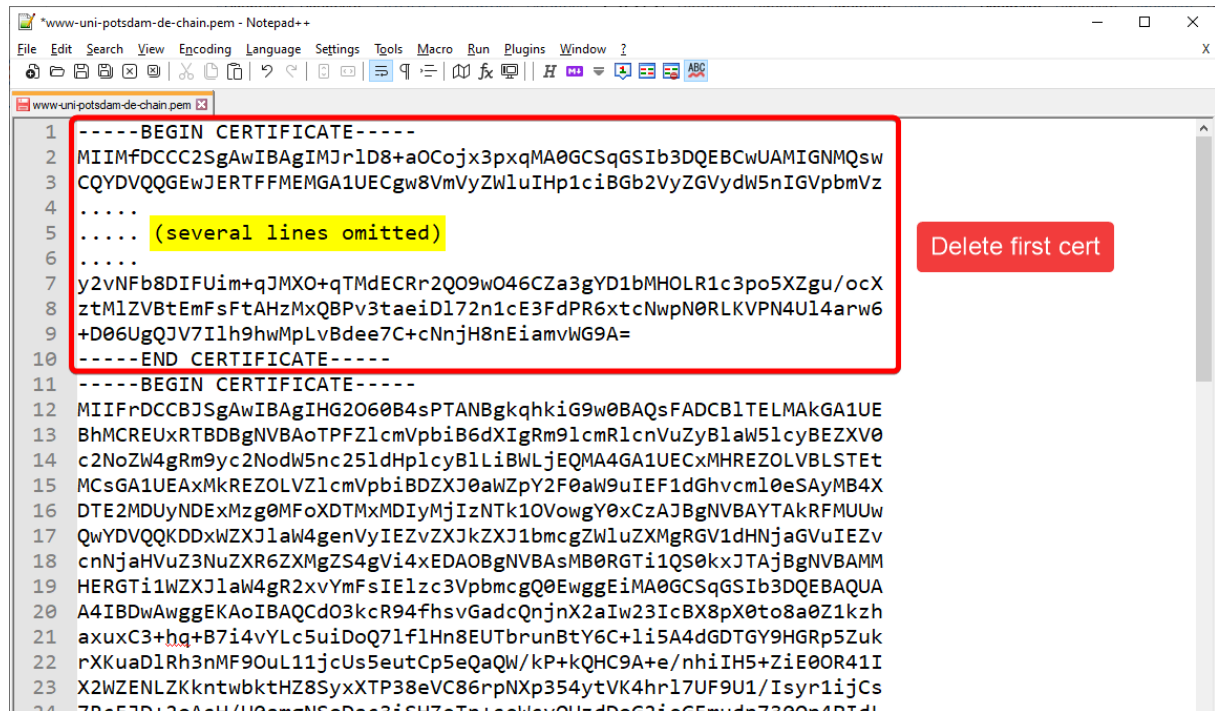




Once the certificate is open, download both the site certificate and the full chain.

Public Key Info	
Algorithm	RSA
Key Size	4096
Exponent	65537
Modulus	A3:A0:7B:98:EF:6C:50:ED:41:CE:CC:2A:30:B1:EA:5C:CA:26:00:22:37:51:9E:3B:60:59...
Miscellaneous	
Serial Number	26:B9:43:F3:E6:8E:0A:88:F1:DE:9C:6A
Signature Algorithm	SHA-256 with RSA Encryption
Version	3
Download	PEM (cert) PEM (chain)
Fingerprints	
SHA-256	42:BC:AE:73:06:15:B5:90:EE:C5:0D:3F:7A:44:DB:B9:7D:A8:DC:6A:E8:C2:E6:5C:BE:C...
SHA-1	83:45:50:48:88:6E:9A:76:23:FF:EA:B3:4B:D1:87:30:79:93:C9:C8

The chain file contains the certificate of current site, plus the certificates of one or more intermediate CAs, all the way up to the trusted root CA. Open the chain file in a text editor and delete the very first certificate (since we already have that in a separate file).



```
1 -----BEGIN CERTIFICATE-----
2 MIIMFDCCC2SgAwIBAgIMJr1D8+aOCojx3pxqMA0GCSqGSIb3DQEBCwUAMIGNMQsw
3 CQYDVQQGEWJERTFFMEMGA1UECgw8VmVvZWluIHp1c1BGB2VyZGVydW5nIGVpbmVz
4 .....
5 ..... (several lines omitted) .....
6 .....
7 y2vNFb8DIFUim+qJMX0+qTmdECRr2Q09w046CZa3gYD1bMHOLR1c3po5XZgu/ocX
8 ztM1ZVBtEmFsFtAHZMxQBPv3taeiD172n1cE3FdPR6xtcNwpN0RLKVPN4U14arw6
9 +D06UgQJV7I1h9hwMpLvBdee7C+cNnjH8nEiamvWG9A=
10 -----END CERTIFICATE-----
11 -----BEGIN CERTIFICATE-----
12 MIIFrDCCBJSgAwIBAgIHG2O6B4sPTANBgkqhkiG9w0BAQsFADCB1TElMAkGA1UE
13 BhMCREUxRTBD8gNVBAoTPFZ1cmVpbiB6dXlIgRm91cmR1cnVuZyBlaw51cyBEZXV0
14 c2NoZW4gRm9yc2NodW5nc25ldHplcyB1LiBWLjEQA4GA1UECzMHRZOLVBLSTETt
15 MCsGA1UEAxMKREZOLVZ1cmVpbiBDZXJ0aWZpY2F0aW9uIEF1dGhvcml0eSAYMB4X
16 DTE2MDUyNDExMzQ0MDUyMjIzNTk1OVowY0xkZjBhbnBAYTAkRFRMUUw
17 QwYDVQQKDDxWZXJ1aw4genVyIEZvZXJkZXJ1bmcgZWluZXNMgRGV1dHNjaGVuIEZv
18 cnNjaHVVZ3NuZXRXZXMgZS4gVi4xEDAOBgNVBAcMB0RGTi1QS0kxJTAjBgNVBAMM
19 HERGTi1WZXJ1aw4gR2xvYmFsIE1zc3VpbmcgQ0EwggEiMA0GCSqGSIb3DQEBAQUA
20 A4IBDwAwggEKAoIBAQCdO3kcR94fhsvGadcQnX2aIw23IcBX8pX0to8a0Z1kzh
21 axuxC3+hq+B7i4vYLC5uiDoQ71f1Hn8EUTbrunBtY6C+li5A4dGDTGY9HGRp5Zuk
22 rXKuaD1Rh3nMF90uL11jcUs5eutCp5eQaQW/kP+kQHC9A+/nhiH5+ZiE0OR41I
23 X2WZENLZKkntwbktHZ8SyxXTP38eVC86rpNXp354ytVK4hr17UF9U1/I5yr1ijCs
24 7B+57D+3aC4H/U0aGmNS0Dac3iS47cTnTc0LayQ1z4DnG3iG5Ewudn730Qn4BTdI
```

Go back the certificate page in Firefox and note down the URL of CA's OCSP responder.

Authority Key ID	
Key ID	6B:3A:98:8B:F9:F2:53:89:DA:E0:AD:B2:32:1E:09:1F:E8:AA:3B:74
CRL Endpoints	
Distribution Point	http://cdp1.pca.dfn.de/dfn-ca-global-g2/pub/crl/cacrl.crl
Distribution Point	http://cdp2.pca.dfn.de/dfn-ca-global-g2/pub/crl/cacrl.crl
Authority Info (AIA)	
Location	http://ocsp.pca.dfn.de/OCSP-Server/OCSP
Method	Online Certificate Status Protocol (OCSP)
Location	http://cdp1.pca.dfn.de/dfn-ca-global-g2/pub/cacert/cacert.crt
Method	CA Issuers
Location	http://cdp2.pca.dfn.de/dfn-ca-global-g2/pub/cacert/cacert.crt
Method	CA Issuers
Certificate Policies	
Policy	Certificate Type (2.23.140.1.2.2)
Value	Organization Validation
...	...

Now we have all the data needed to send a query to that OCSP server. For this purpose, we will use the well-known **openssl** utility. It is available pre-installed on most Linux distributions.

Windows users can get it by setting up a Linux virtual machine OR through [Git for Windows](#) (launch Git Bash, it includes openssl command).

Mac users can get it via Homebrew: `brew install openssl`.

Once installed, send the query to OSCP server using following command, replacing the parts in red with correct file names and URL.

```
openssl ocsp -issuer chain.pem -cert cert.pem -url  
http://ocsp.pca.dfn.de/OCSP-Server/OCSP
```

In the response, look for the following lines to know the status:

```
cert.pem: good  
      This Update: Sep 26 07:46:48 2024 GMT  
      Next Update: Oct  3 07:46:47 2024 GM
```

Deliverables

Attempt the following tasks/questions.

1. Mention your chosen website. Check its certificate status as above. Show the screenshots of your OCSP query and response.
2. In case the OCSP responder is down (or not reachable), the certificate status cannot be checked. How do the web browsers handle this situation? Do you think their handling is adequate from security point of view?
3. Theoretically, the OCSP server can also be compromised. How can the client ensure integrity and authenticity of an OCSP response?
4. Can you think of any privacy concerns in OCSP mechanism? Read about 'OCSP stapling' and discuss how that eliminates those privacy problems.
5. OCSP usage on the Internet is declining. A very well-known free certificate provider Lets Encrypt has [recently announced](#) their intention to stop offering OCSP. The most popular web browser, Google Chrome does not support OCSP at all! Firefox is also experimenting with other revocation checking methods. Find out what methods are being adopted in modern browsers, and what are their merits and demerits compared to OCSP.

4 + 4 + 4 + 6 + 6 marks