Auto-Evaluation Questions
(X509 Authentication, X509v3 Certification and PKIs)

1. What is a public-key directory and what are the main ingredients of a public-key directory?
2. What is a public-key certificate?
3. What are the requirements for the use of a public-key certificate scheme?
4. What is the purpose of the X.509 standard?
5. What is a certification chain?
6. How is an X.509 certificate revoked?

   - - -
7. What is a certificate in a CSR format? (Certificate Signed Request) ?
8. Try to obtain a certificate from a TLS (or SSL) connection with your browser. Open the certificate and interpret the different attributes in the different fields of the certificate, as well as the structure of the certificate
9. Try to obtain a certificate revocation list from a CRL endpoint of a certificate obtained in a TLS connection (using your browser). What is the organization and internal structure of the CRL? What is in each entry of the CRL? What type of signature was used for the CRL issuing?

   Hint: remember that you can also see the CRL structure using the keytool of your java installation.
10. What is the difference between forward certificates and reverse certificates in the processing of a certificate chain?
11. What is the meaning of the following attributes in a X509v3 certificate
    a. Authority Key Identifier
    b. Subject Key Identifier
    c. Key usage
    d. Private-Key usage period
    e. Certificate Policies
    f. Policy Mappings
12. Given a X509v3 certificate, present and describe the purpose of the Subject and Issuer Attributes
13. Describe some constraints that can be present in a X509v3 certificate
14. What is a PEM format for a public-key certificate X509v3 ? What is the main difference compared with other formats ?
15. Describe other formats you know that can be used to support X509v3 certificates.
16. Give an example of a Policy constraint that must be used to not allowing a certain certificate to be sued as a CA certificate or a certificate that cannot be used to validate signatures for issuing other certificates
17. If you look to the fingerprint field in a conventional X509v3 certificate, two different hash functions are included in the fingerprints' attributes. Why? (See for example the certifiates in a a certification chain form www.google.com) that includes SHA-1 and SHA-256 hash results.

18. Complementarity to the question 17, why SHA-1 or MD5 are usually chosen as one of the hash-functions in the fingerprints?
19. In a X509v3 certificate, how do you know that the certified public key can be used to validate signatures, signing other issued certificates?
20. If a signer wants to sign a message with RSA-PKCS#1 or RSA-PSS, is it possible to have a X509v3 certificate certifying her/his RSA public key and presenting together with the signature a certification chain, in which the certificates in upper levels are all certificated of DSA public keys?
21. A Two-way or mutual authentication and key-distribution can be implemented with the following message exchanges between Alice (A) and Bob (B):

    Exchange 1:

    A>B: [{ta, ra, IdB}Kab, {Kab}KpubB], signDataA, Certificattion Chain
    B>A: [{tb, ra+1, rb, IdA}Kba, {Kba}KpubA], signDataB, Certificattion Chain

    Exchange 2:

    A>B: [{ta, ra, IdB}Kab, signData, {Kab}KpubB], Certificattion Chain
    B>A: [{tb, ra+1, rb, IdA}Kba, signData, {Kba}KpubA], Certificattion Chain
    A>B: {rb+1}Ks

ta, tb:	timestamps
ra, rb:	challenge-nonces (with the respective responses ra+1, rb+1)
IdA, IdB:	Unique identifiers for Alice and Bob
KpubA, KpubB:	Publie Keys of A and B, certified with a correct forward certification chain, where the root-level certificate is trusted for A and B
Ks:	Established session (symmetric) key, generated in the following way: Ks = SHA-256(Kab ‖ Kba) // ‖ means concatenation
Kab, Kba:	Pre-master keys generated by Alice and Bob respectively
SignDataA	Signature of message […] sent by Alice to Bob
SignDataB	Signature of message […] sent by Bob to Alice

    Question: What is the advantage of Exchange B compared wit Exchange A if both implement mutual authentication ?

22. Use the openssl tool in the following way:

```
openssl s_client -connect www.bpi.pt:443
```

Looking to the obtained certification chain explain:

- What is the root-level certificate ?
- What is the type of chain ? Is it a reverse or a forward chain ?
- How many levels you have in the chain ?
- What is the root-level CA in the obtained chain ?
- What is the private/public key and algorithm used by the server www.bpi.pt and what is the size of such keys?

23. What means OID (Object identifiers), expressed in some attributes that can appear in a X509v3 certificate?
24. What is an EV (Extended Validated) Certificate? What is different with no EV Certificates?
25. Theoretically, CRLs can be used in different management ways: White List CRLs, Black List CRLs, Full-URLs, Incremental URLs, Time-Controlled URLs or Version-Controlled URLs. Using your browser to analyze the certificate of CLIP, what type of CRL management is done, from the certificate issuer ?
26. What is the transport protocol used by the OCSP Protocol ? Is it TCP or UDP ?
27. How do you define a PKI?
28. What is the difference between a Registration Authority (RA) and a Certification Authority (CA) in the PKIX Architectural model?
29. Giving the PKIX model, what entity is responsible for issuing CRLs ?
30. Why in the PKIX Architectural model it is required a Cross-Certification support?
31. In the PKIX model and management functions and protocols, what is the scope (objective) and the role of the following protocols:
    a. CMP – Certificate Management Protocols
    b. CMS – Certificate Management Syntax
    c. OCSP