uc3m | Universidad **Carlos III** de Madrid

CRYPTOGRAPHY AND COMPUTER SECURITY

Ana I. González-Tablas Ferreres
José María de Fuentes García-Romero de Tejada
Lorena González Manzano
Sergio Pastrana Portillo
UC3M | GRUPO COMPUTER SECURITY LAB (COSEC)

“Public key infrastructures”

Self-assessment test

Select the correct answer.

1. A public key certificate:

   ○ Certifies that certain public key is linked to certain private key.
   ○ **Certifies that certain public key is linked to certain entity.**
   ○ Certifies that certain private key is linked to certain symmetric key.
   ○ Certifies that certain private key is linked to certain entity.

2. If the state of a public key certificate…:

   ○ …is “valid”, we can trust in the relation it certifies forever.
   ○ …is “revoked”, we can trust in the relation it certifies only during the validity period stated in the certificate.
   ○ **…is “revoked”, we cannot trust in the relation it certifies from the time it has been revoked.**
   ○ …is “revoked”, we cannot trust in the relation it certifies at any time.

3. Let’s assume the following hierarchy of ACs: ACR is the root certification authority, AC1 and AC2 are two subordinate certification authorities, A is an end-user of AC1 and B is an end-user of AC2. If A receives B’s certificate, she has to verify the validity of the certificates of the following authorities:

   ○ Only ACR and AC2.
   ○ Only ACR and AC1.
   ○ All: ACR, AC1 and AC2.
   ○ **Only AC2.**

4. When validating the state of a certificate:
    - **Certificate Revocation Lists (CRL) is a valid method but it presents some problems given its need of a high bandwidth.**
    - It is recommended that Revocation Authorities update Certificate Revocation Lists (CRL) every time they revoke a certificate.
    - Certificate Revocation Lists (CRL) allow to know at any time the validity state of a certificate.
    - Certificate Revocation Lists (CRL) are published encrypted and accessing them requires owning a public key certificate from that Public Key Infrastructure.

5. A Revocation Authority publishes an update of the Certificate Revocation List (CRL) every day at 23:59:59 hours:minutes:seconds. Let's assume that the last CRL was published on the day X, and while in day X+1, we receive a certificate that we have to validate to verify a digital signature generated that same day X+1. We can trust in…:
    - …the certificate is "valid", if it is not in the CRL published in day X, assuming that the validity period of the certificate includes day X+1.
    - …the certificate will be "valid", if it does not appear in the CRL that will be published on day X+1, independently of whether its validity period includes day X+1 or not.
    - **…the certificate will be "valid", if it does not appear in the CRL that will be published on day X+1, assuming that the validity period of the certificate includes day X+1.**
    - …the certificate is "valid", if it is not in the CRL published in day X, independently of whether its validity period includes day X+1 or not.

6. Comparing hierarchical and decentralized models of Public Key Infrastructures:
    - In the decentralized model no one certifies the public keys.
    - In the hierarchical model an end user can choose to trust or not the certificate of another end-user.
    - **In the hierarchical model, an end user can choose to trust or not the certificate of a Root Certification Authority.**
    - The combination of the hierarchical model with the decentralized model, known as hybrid model, offers more advantages in relation to scalability.