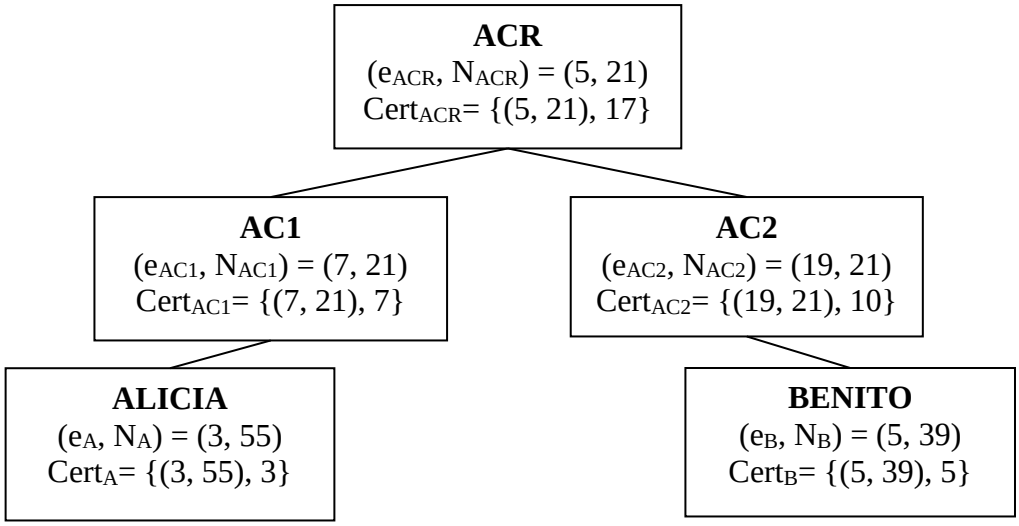
Ana I. González-Tablas Ferreres
José María de Fuentes García-Romero de Tejada
Lorena González Manzano
Sergio Pastrana Portillo
UC3M | GRUPO COMPUTER SECURITY LAB (COSEC)

# "Public key infrastructures"

## Proposed exercises

**Exercise 1:**

Alicia wants to send a signed message to Benito. The certification authorities' hierarchy and the public key and public key certificates in use are shown in the following figure.




Considerations:

- The certificate of an entity *i* consists of her public key and the signature on the public exponent of the public key issued by the certificate issuer. That is, $Cert_i = \{(e_i, N), S_{issuer}(e_i)\}$, being $S_{issuer}(e_i)$ the RSA signature generated by the certificate issuer (the entity immediately precedent within the shown hierarchy).
- Root certification authority self-signs her certificate.
- No hash functions are used.
- Each entity owns a local copy and trust the certificates within the certificate chain of her own certificate (e.g., Benito owns $Cert_{AC2}$ and $Cert_{ACR}$, and he trusts the local copy of their certificates).

Answer the following questions:

**a)** Compute Alice's RSA signature of message M = 2.

**b)** What should send Alicia to Benito so he can check that the message was sent by Alicia? Argument your answer.

**c)** Assuming that Alicia sends Benito {M, $S_A(M)$, $Cert_A$, $Cert_{AC1}$, $Cert_{ACR}$}, being M = 2 and $S_A(M)$ the result computed in question a), show ALL the computations that Benito should perform to check the authenticity of the received message.

**Exercise 2 :**

Alice wants to send to Benito a message M signed with RSA. The public keys of Alice and Benito are certified by the certification authorities $CA_A$ and $CA_B$ respectively. A third certification authority (CA) exists, that certifies $CA_A$ and $CA_B$. Consider that the three certificates are only composed of the signature of the public key exponent of the subject of the certificate.

Data:

- All certification authorities have the same modulo: N=55
- AC public key is ($e_{CA}$, N)=(7, 55)
- Public exponents of $AC_A$ and A are not provided
- $AC_A$ 's public key is $(e_{CA_A}, N) = (e_{CA_A}, 55)$
- A's public key is ($e_A$, N)=($e_A$, 55)
- The certificate of $CA_A$ issued by CA is 8
- The certificate of A issued by $AC_A$ is 7

Questions:

a) Calculate the public key of CAA.

b) Calculate the public key of A.

c) Consider the public key of A is ($e_A$, N) = (49, 55), compute the RSA signature on the message M=4 by Alice.