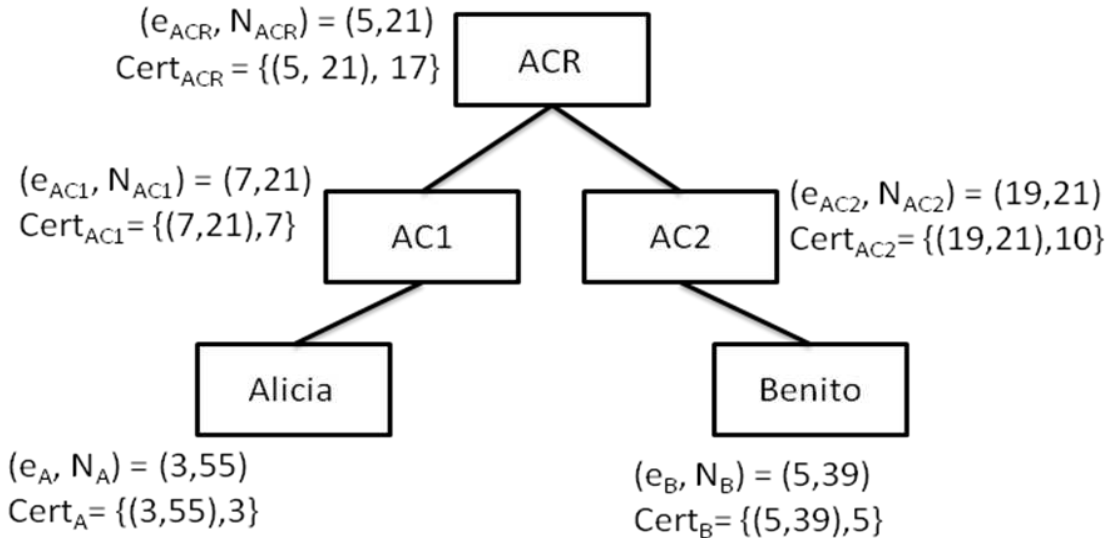
EJEMPLO de PROBLEMA DE EXAMEN (1.25 *puntos*)

Alicia quiere mandar un mensaje firmado a Benito. La jerarquía de autoridades de certificación y las claves públicas y certificados en cuestión son los que se muestran en la figura a continuación.



Teniendo en cuenta las siguientes consideraciones:

- El certificado de cada entidad *i* está compuesto por su clave pública y la firma del exponente de esa clave pública por parte de la entidad emisora del certificado, es decir, $Cert_i = \{(e_i,N_i), F_{emisor}(e_i)\}$, siendo F_{emisor} la firma RSA realizada por la entidad emisora del certificado (entidad inmediatamente superior).
- La autoridad raíz ACR firma su propio certificado.
- No se usan funciones resumen.
- Cada entidad posee y confía en los certificados de toda su cadena de certificación (ej: Benito posee los certificados de AC2 y ACR y además confía en ellos).

a) Calcule la firma RSA del mensaje M=2 realizada por Alicia.

b) ¿Qué tendrá que enviar Alicia a Benito para que éste pueda comprobar que el mensaje fue enviado por Alicia? Justifique su respuesta.

c) Suponiendo que Alicia le envía a Benito $\{M, F_A(M), Cert_A, Cert_{AC1}, Cert_{ACR}\}$. Realice TODOS los cálculos que tendría que realizar Benito para comprobar la autoría del mensaje enviado (M=2).