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

"Infraestructuras de clave pública"

Test de autoevaluación

Seleccione la respuesta correcta.

1. Un certificado de clave pública:
   - o Acredita que cierta clave pública está asociada a cierta clave privada.
   - o **Acredita que cierta clave pública está asociada a determinada entidad.**
   - o Acredita que cierta clave privada está asociada a cierta clave simétrica.
   - o Acredita que cierta clave privada está asociada a determinada entidad.

2. Si el estado de un certificado de clave pública…:
   - o …es "válido", se podrá confiar en la relación que acredita para siempre.
   - o …es "revocado", se puede confiar en la relación que acredita solo durante el periodo de validez del certificado.
   - o **…es "revocado", ya no se puede confiar en la relación que acredita a partir de la fecha de revocación.**
   - o …es "revocado", ya no se puede confiar en la relación que acredita en ningún momento temporal.

3. Asumimos que existe cierta jerarquía de autoridades de certificación estructuradas de la siguiente manera: ACR es la autoridad de certificación raíz, AC1 y AC2 son dos autoridades de certificación subordinadas, A es un usuario final de AC1 y B es un usuario final de AC2. Si A recibe e, certificado de B, debe verificar la validez de los siguientes certificados:
   - o Solo ACR y AC2.
   - o Solo ACR y AC1.
   - o Todos: ACR, AC1 y AC2.
   - o **Solo AC2.**

4. En relación con la validación del estado de un certificado:
   - **Las Listas de Certificados Revocados (CRL) es un metodo válido pero acarrea numerosos problemas de consumo de ancho de banda.**
   - Se recomienda que las Autoridades de Revocación actualicen las Listas de Certificados Revocados (CRL) con cada certificado que pasa a estar revocado.
   - Las Listas de Certificados Revocados (CRL) permiten conocer en cualquier momento el estado de la validez de un certificado.
   - Las Listas de Certificados Revocados (CRL) se publica cifrada y es necesario contar con un certificado de dicha Infraestructura de Clave Pública para poder acceder a dicha CRL.

5. Una Autoridad de Revocación publica la actualización de su Lista de Certificados Revocados (CRL) todos los días a las 23:59:59 horas:minutos:segundos. Si la última CRL se publicó el día X, y estando en el transcurso del día X+1 recibimos un certificado que debemos validar para verificar una firma digital generada el mismo día X+1, podemos confiar en que el certificado…:
   - …es "válido", si no aparece en la CRL publicada en el día X, supuesto que su periodo de validez incluye el día X+1.
   - …será "válido", si no aparece en la CRL que se publicará en el día X+1, independientemente de si su periodo de validez incluye o no el día X+1.
   - **…será "válido", si no aparece en la CRL que se publicará en el día X+1, supuesto que su periodo de validez incluye el día X+1.**
   - …es "válido", si no aparece en la CRL publicada en el día X, independientemente de si su periodo de validez incluye o no el día X+1.

6. Comparando el modelo jerárquico con el modelo descentralizado de las Infraestructuras de Clave Pública:
   - En el modelo descentralizado nadie certifica las claves públilcas.
   - En el modelo jerárquico un usuario puede decidir si confía o no en el certificado de cierta entidad final.
   - **En el modelo jerárquico un usuario puede decidir si confía o no en el certificado de cierta Autoridad de Certificación Raíz.**
   - La combinación del modelo jerárquico con el descentralizado, conocido como modelo híbrido, es la que más ventajas ofrece en relación a la escalabilidad.