Práctica 6: Claves

1. Ejercicio 1

Preguntas

1. Explica si el nodo receptor del mensaje Z puede o no descifrar el mensaje para acceder a su contenido.

Si, porque la única forma de descifrar el mensaje es con la clave privada de z. Y esta solo la posee el destinatario Z

2. Explica si el nodo receptor del mensaje Z estar seguro de la confidencialidad del mensaje, es decir, de que ningún otro nodo ha podido descifrarlo.

Sería un mensaje totalmente confidencial porque para descifrarlo se necesita la clave privada de z y no la tiene nadie

3. Explica si el nodo receptor del mensaje Z puede autenticar al nodo emisor del mensaje X.

Si puede, ya que en el contenido del mensaje esta la dirección del emisor.

4. Explica si el nodo receptor del mensaje Z puede estar seguro de la integridad del mensaje, es decir, que ningún otro nodo ha podido alterar el contenido del mensaje.

Ningún otro ha podido alterarlo, ya que se necesita la clave privada de z para descifrarlo.

5. Explica si un nodo cualquiera que intercepte un mensaje destinado al nodo Z puede conocer el texto del mensaje ParaZ.

No podría porque no dispone de la clave privada.

6. Explica si un nodo cualquiera que intercepte un mensaje destinado al nodo Z puede conocer el destino final del mensaje.

Se podría ver analizando la secuencia de nodos.

7. Explica si un nodo cualquiera que intercepte un mensaje destinado al nodo Z puede conocer el nodo que creó el mensaje

No podría ya que por ejemplo el nodo d tampoco sabe quién creo el mensaje, solo sabe quién se lo envió a él, pero no sabe si es el creador.

2. Ejercicio 2

Preguntas

1. Indica cómo crees que debería enviarle la clave Ks de Alicia a Roberto.

Alicia debería establecer la clave publica de Roberto a la clave simétrica. Y a su vez debería establecerle la clave simétrica al mensaje. De esta forma Roberto desbloqueara la clave simétrica con su clave privada, y el mensaje con la clave simétrica.

2. Alicia no tiene la clave pública de Roberto ni Roberto la de Alicia. Indica cómo podría conseguir Alicia la K + R, sin quedar físicamente para intercambiarse las claves, y como puede Alicia estar segura de que esta clave se corresponde con la de Roberto.

Podrían pedir a un tercero de confianza que les pase la clave publica de alguno de ellos.

3. ¿Con este sistema, puede estar Alicia segura de que los mensajes que envía a Roberto son confidenciales y de que en realidad se está comunicando con Roberto? En caso negativo, explica cómo conseguirías estas propiedades en los mensajes enviados desde Alicia a Roberto.

Segura al 100% no podría estar, ya que la única forma de saber que la clave publica es la de Roberto es que se la del propio Roberto. De esta forma usando un tercero de confianza te estas arriesgando a que te de su clave personal y diga que es de Roberto, de esta forma le estarías enviando los mensajes al tercero y no a Roberto.

La forma de saber que la clave de Roberto es la suya, seria dándola en persona o con las Autoridades de Certificación. Esta autoridades ven que esa clave pertenece a Roberto, y la firman y señan como certificado digital.

4. Con este sistema, ¿puede estar Roberto seguro de que los mensajes son confidenciales y provienen de Alicia? En caso negativo, explica cómo conseguirías estas propiedades en los mensajes enviados desde Alicia a Roberto.

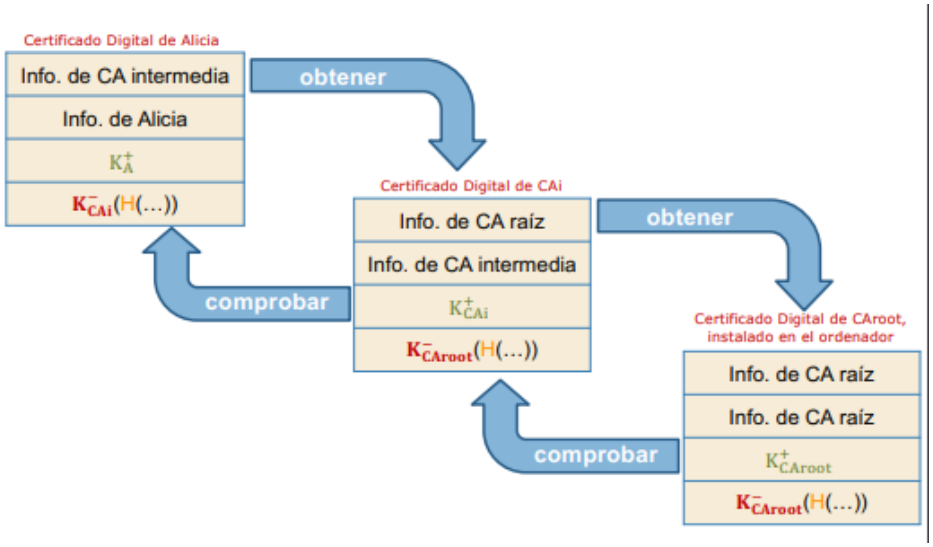
No es del todo seguro ya que puede que al obtener la calve pública no sea del todo segura, para ello se crean un sistema jerárquico de 3 niveles.

- Certificados de entidades finales: Emitidos por CAs intermedias.
- CAs intermedias: certifican las claves públicas de las entidades finales. Sus certificados son emitidos por CAs raíz.
- CAs raíz: certifican las claves públicas de las CAs intermedias. Sus certificados son emitidos por ellas mismas.

5. El certificado de la clave publicada de Roberto ha caducado y ya no es válido. Roberto decide cambiar de autoridad de certificación y consigue un certificado de su clave pública emitido por la autoridad de certificación CA3. Esta autoridad de certificación CA3 no ha incluido su certificado autofirmado en las aplicaciones de comunicaciones del sistema, pero CA3 tiene un certificado de la clave pública de CA3 firmado por CA2. Indica si ahora Alicia podría enviar a Roberto mensajes confidenciales y auténticos y explica cómo lo haría.

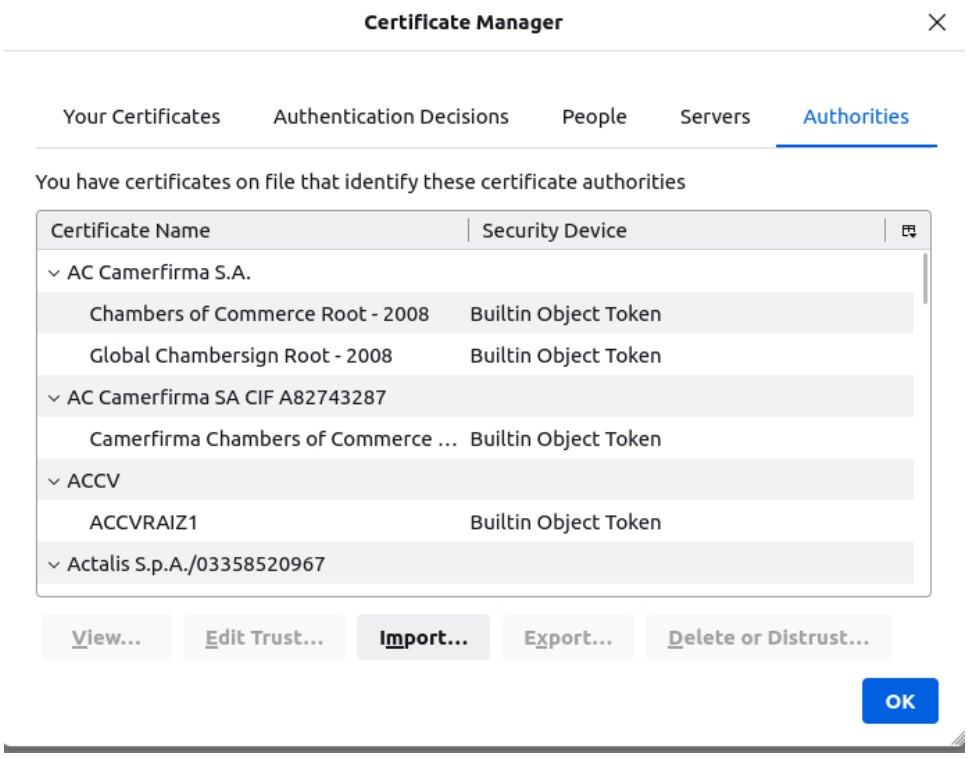
Si seria de forma confidencial y autentica.

Se haria de esta forma y estabbleciendo estas claves publicas:

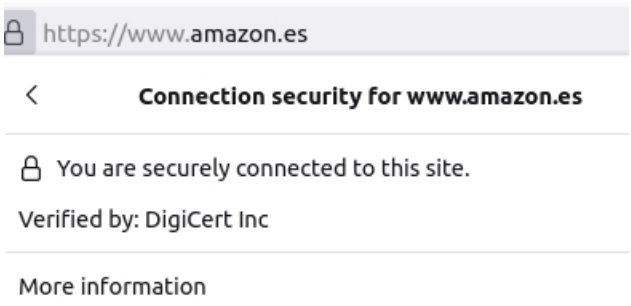


3. Ejercicio 3

En la pestaña ´´Autoridades´´ verás los certificados de las autoridades de certificación de primer nivel

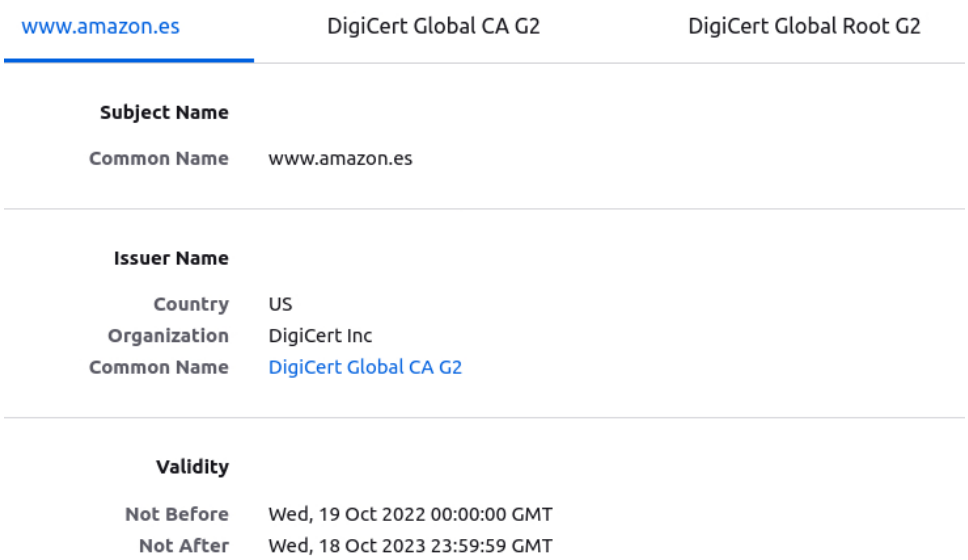


1. Escribe en la URL del navegador la siguiente dirección: www.amazon.es, una vez que se haya cargado la página verás junto a la URL un candado verde, pulsa sobre él y luego sobre la flecha derecha al lado de ´´Conexión segura´´ (´´Mostrar detalles de la conexión´´). Indica cuál es la autoridad de certificación que ha verificado esta conexión segura.



Ha sido verificada por DigiCert Inc.

2. En esa ventana de detalles de la conexión, pulsa sobre el botón Más información y luego en ´´Ver Certificados y en la pestaña "Detalles". Indica cuál es la jerarquía de certificados que se está utilizando para verificar a Amazon.



Selecciona empezando por www.amazon.es el campo ´´Emisor´´ y ve comprobando quiénes han sido las entidades que han generado los certificados que aparecen en la jerarquía. Comprueba la cadena de todos los certificados. Señala qué certificados de la jerarquía están autoafirmados

3. Vuelve a visitar la información de certificados de las Preferencias (Editar → Preferencias → Privacidad y Seguridad → . . .→ Ver Certificados). Observarás que las dos entidades que aparecen en la jerarquía de certificados de Amazon tienen instalado su certificado. Una de ellas muestra su certificado como Builtin object token, es decir, se trata de un certificado autofirmado de una autoridad de certificación raíz que venía instalado con la aplicación Firefox. El otro certificado se

muestra como Disp. software de seguridad, por lo que no es un certificado autofirmado y la entidad que lo ha firmado es una autoridad de certificación raíz. Indica cuál de ellos es Builtin object token y cuál es Disp. software de seguridad