Tema 3 – Protocolos y mecanismos de seguridad

1 GESTIÓN DE LAS CLAVES

1.1 PROTOCOLOS DE DISTRIBUCIÓN DE CLAVES SIMÉTRICAS

La criptografía híbrida presenta problemas de escalabilidad, es por ello que necesitamos una entidad que distribuya de forma centralizada las claves, la cual puede ser TTP (Trusted Third Party) / KDC.

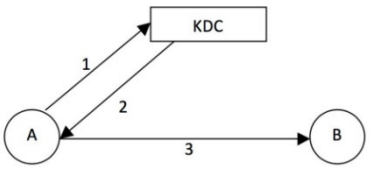
El sistema se basa en dos clases de claves, las del canal cifrado con la TTP y la de ambos. Es necesario tener acceso a un servidor común de confianza.

Los modelos de distribución pueden ser:

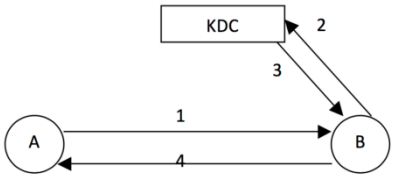
- Simple ("**La Rana de la Boca Grande**"):
  - Está expuesto a un replay attack y consiguiente Denegación de Servicio que pudiera ser solventado mediante:
    - Marcas de tiempo, para descartar mensajes obsoletos (con problemas de sincronización).
    - Nonce / único (no-único), como número aleatorio no único que no debería repetirse (si no se pierde la lista de números) y que permitiría descartar mensajes con mismo nonce.

1.1.1 Modelos Genéricos de KDC

- PULL
  - A -> KDC, A solicita la clave de sesión K_{AB} con un valor N1 (sello de tiempo).
  - KDC -> A, el KDC le contesta con un mensaje cifrado de K_{AT} con la clave de sesión
  - A -> B, A envía a B la clave cifrada con K_{BT} (cifrada por KDC).
  - Desafío-Respuesta
    - B -> A, se genera otro nonce (aleatorio) y envía cifrado con la clave.
    - A -> B, se devuelve nonce – 1 y envía cifrado con la clave.



- PUSH
  - A -> B, se solicita un canal seguro
  - B -> KDC
  - KDC -> B
  - B -> A, se reenvía la solicitud a A para que obtenga K_{AB}



1.1.2 Protocolo de Needham-Schroeder - PULL

1. $A \rightarrow T: A, B, N_A$
2. $T \rightarrow A: \{R_A, B, K_{AB}, \{K_{AB}, A\}_{K_{BT}}\}$
3. $A \rightarrow B: \{K_{AB}, A\}_{K_{BT}}$
4. $B \rightarrow A: \{N_B\}_{K_{AB}}$
5. $A \rightarrow B: \{N_B - 1\}_{K_{AB}}$

Puede suplantar el a Alice, Bob si tiene una de las claves con T. Pero también puede atacar por denegación de servicio, algo que se podría resolver extendiendo el uso de nonce.

1.1.3 Protocolo de Ammended Needham-Schroeder - PULL

Resuelve el problema de denegación de servicio

1.1.4 Protocolo de Otway-Rees - PUSH

1. $A \rightarrow B: I, A, B, \{R_A, I, A, B\}_{K_{AT}}$
2. $B \rightarrow T: I, A, B, \{R_A, I, A, B\}_{AT}$
3. $T \rightarrow B: I, \{R_A, K_{AB}\}_{AT}, \{R_B, K_{AB}\}_{BT}$
4. $B \rightarrow A: I, \{R_A, K_{AB}\}_{K_{AT}}$

Si la longitud de K_{AB} coincide con la concatenación de $I + A + B$ un atacante podría interceptar y sería posible reenviar el mensaje como $I, E_{AT}(R_A, K_{AB}) \equiv I, \{R_A, I + A + B\}_{K_{AT}}$, pudiendo suplantar a Trent o Bob.

1.1.5 Protocolo Kerberos - PULL

En este algoritmo se crea un timestamp como un tiempo de vida:

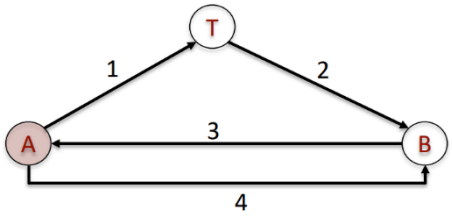
1. $A \rightarrow T: A, B$
2. $T \rightarrow A: \{T, LB, K_{AB}, A\}_{BT}, \{T, LB, K_{AB}, B\}_{AT}$
3. $A \rightarrow B: \{A, T\}_{K_{AB}}, \{T, LB, K_{AB}, B\}_{AT}$
4. $B \rightarrow A: \{T + 1\}_{K_{AB}}$

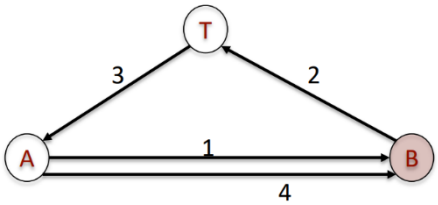
Se utiliza en la autenticación en varios servidores de forma simultánea. Asume sincronización de relojes y fallos del sistema podrían generar ataques DDOS

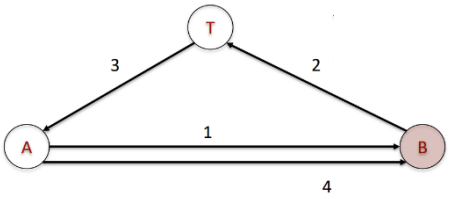
1.1.6 Protocolos extendidos

Existen mecanismos de seguridad que expanden PULL y PUSH:

- PULL EXTENDIDO
  - $A \rightarrow KDC$
  - $KDC \rightarrow B$
  - $A \rightarrow B$
  - $B \rightarrow A$
- PUSH EXTENDIDO
  - $A \rightarrow B$
  - $B \rightarrow KDC$
  - $KDC \rightarrow A$
  - $A \rightarrow B$







1.1.7 Yahalom – PUSH EXTENDIDO

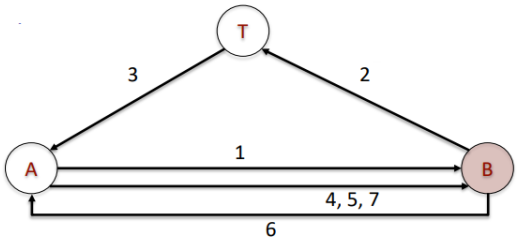
- $A \rightarrow B: A, N_A$
- $B \rightarrow T: B, \{A, N_A, N_B\}_{K_{BT}}$
- $T \rightarrow A: \{B, KAB, Na, Nb)_{K_{AT}}, \{A, KAB\}_{K_{BT}}$
- $A \rightarrow B: \{A, K_{AB}\}_{K_{BT}}, \{N_B\}_{K_{AB}}$

1.1.8 Neuman Stubblebine – PUSH EXTENDIDO

Combina time-stamps con nonces.

- $A \rightarrow B: A, N_A$

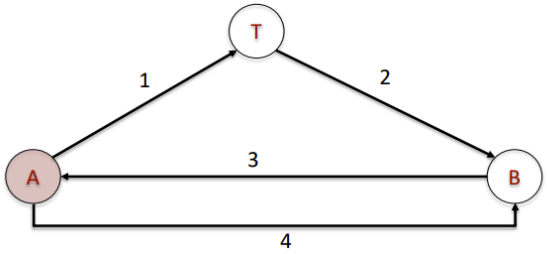
- $B \rightarrow T: B, N_B, \{A, N_A, t_b\}_{K_{BT}}$
- $T \rightarrow A: \{B, K_{AB}, N_A, t_B\}_{K_{AT}}, \{A, K_{AB}, t_B\}_{K_{BT}}, N_B$
- $A \rightarrow B: \{A, K_{AB}, t_b\}_{K_{BT}} \{N_B\}_{K_{AB}}$
- $A \rightarrow B: N'_A, \{A, K_{AB}, t_b\}_{K_{BT}}$
- $B \rightarrow A: N'_B, \{N'_A\}_{K_{AB}}$
- $A \rightarrow B: \{N'_B\}_{K_{AB}}$



1.1.9 Kao Chow (cachau) – PULL EXTENDIDO

Usa solo nonces.

- $A \rightarrow T: A, B, N_A$
- $T \rightarrow B: \{N_A, K_{AB}, A, B\}_{K_{AT}} \{N_A, K_{AB}, A, B\}_{K_{BT}}$
- $B \rightarrow A: \{N_A, K_{AB}, A, B\}_{K_{AT}}, \{N_A\}_{K_{AB}}, N_B$
- $A \rightarrow B: \{N_B\}_{K_{AB}}$



1.1.10 Problemas de KDC

- El KDC posee información como para **suplantar** a cualquier usuario.
- Es un único **punto de fallo**
- El rendimiento de todo el sistema puede bajar cuando el KDC se convierte en el **cuello de botella**.

1.2 MECANISMOS E INFRAESTRUCTURAS DE ADMINISTRACIÓN DE CLAVES PÚBLICAS

1.2.1 Certificados Digitales

Los certificados digitales hacen de sello de garantía sobre una clave pública de una entidad; este documento digital puede contener:

- La identidad del usuario
- El valor de la clave pública
- Número de serie (identificador)
- Fecha de emisión y expiración
- La identidad de quien emite el documento
- La firma digital de quien emite el documento

1.2.2 Autoridades de Certificación

La Autoridad de Certificación es una TTP que administra los certificados digitales de los usuarios de un sistema.

La ITU-T ha definido una estructura estándar de certificado digital adoptada internacionalmente, el certificado X.509 (versión, número de serie, algoritmo de firma, emisor, periodo de validez, sujeto, algoritmo de clave pública (V1), identificador único

emisor e identificador único de usuario (V2), extensiones (V3 y la firma de la CA). Al generarse, se exportan en formato PKCS#12 (RFC7292).

La firma digital contiene el valor hash del conjunto de los demás campos del certificado.

Como CA debería permitirse que el certificado permita la firma digital, firmar certificados y CRL sign, para revocar los certificados si quedan expuestos).

1.2.3 Tipos de Certificados Digitales

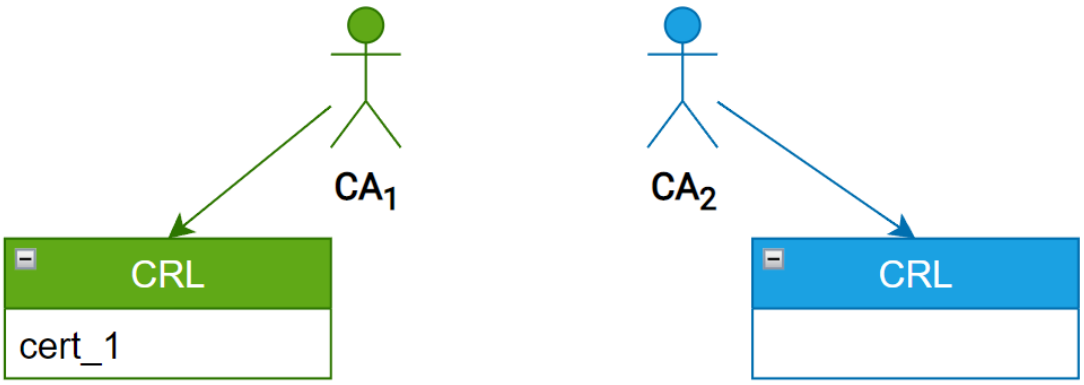
Los certificados pueden estar firmados por una CA o autofirmados.

1.2.4 Infraestructura de Clave Pública (PKI)

Ofrecen los servicios esenciales de:

- Emisión de certificados
- Distribución de certificados
- Obtención de certificados
- Certificación cruzada
- Generación de claves
- Actualización de claves
- Salvaguarda y recuperación de calves
- Revocación y suspensión de certificados.

1.2.5 El problema de las CRLs



Cada CAs emiten CRLs regularmente según su política de certificación, cuando se alcanza la fecha de expiración, se eliminarán de la CRL. Para autenticar la CRL, estas vienen firmadas por las CAs también. En la versión 2 de x.509 se incluye la actualización presente y futura.

Debido a que las CRLs tardan algo en distribuirse entre las Cas, existe un protocolo OCSP, Online Certificate Status Protocol, donde un servidor de **alta disponibilidad** (**en cualquier localización**), que verifique el estado del certificado.

1.2.6 Tarjetas inteligentes

Las tarjetas inteligentes o smartcard son tarjetas que incluyen un chip donde se puede almacenar información o incluso realizar complejos cálculos criptográficos; pueden ser clasificadas como tarjetas:

- De contacto

- Sin contacto (contactless)

, o por sus capacidades, tarjetas de memoria, microprocesadas o criptográficas…

El DNI electrónico ofrece una retención de al menos 10 años y contiene módulos de aceleración para algoritmos de claves públicas y privadas y cuenta con un sistema operativo DNIe v3.0. El DNIe contiene tanto un certificado de autenticación (identidad y acceso seguro) como de firma digital (firma de documentos), además cuenta con un certificado de componente para la interconexión de los componentes (evitando la emulación). Tiene un generador interno de número aleatorios para la generación de claves.

La memoria EEPROM se divide en tres zonas, **pública** (certificado CA, claves DH, certificado X.5090, **privada** (certificado de autenticación y certificado de firma) y de **seguridad** (datos de filiación, fotografía del titular, imagen de la firma manuscrita), que se puede acceder en los puntos de actualización del DNI-e.

Como con los certificados digitales, es posible revocar el DNI con un OCSP.

Además, se separan las responsabilidades con funciones **Autoridad de Validación**, con el único propósito de validar.

1.3 Mecanismo de autenticación

Podemos clasificar tres formas en los que clasificar los mecanismos de autenticación.

- Sólo yo conozco (contraseñas)
  - Más de un usuario puede usarla a la vez se pueden pasar entre usuarios (aunque debería no transferirse).
  - Requiere de políticas de seguridad, renovación, robustez…
  - **En en un sistema la base de datos las contraseñas deben tener cifradas.**
- Sólo yo tengo (clave privada, tokens, certificados)
  - Un objeto físico prueba tu identidad.
  - Siendo físico podría usarlo.
  - Son clonables y con posibilidad de perder la autenticación del original.
- Sólo yo soy (autenticación biométrica)
  - Muy difícil de traspasar o suplantar
  - Se requieren requisitos de protección especiales (Ley de Protección de Datos), más caros, aunque siguen pudiéndose clonar en algunos casos.

1.3.1 Salt

La sal es un condimento que añadir a la sal para evitar conseguir coincidencias de hashes y contraseñas (dificulta los ataques de diccionarios con las contraseñas más comunes password, 123456789…). Se añade como valor aleatorio único por cada usuario que se concatena a la clave original.

- Nunca reutilizar
- Suficientemente larga, min 57 bits
- Funciones hash lentas para evitar ataques de fuerza bruta

1.3.2 Autenticación de doble factor

Supone la combinación de uno de los métodos anteriores; por parte de los servicios de pago, en la UE es obligatoria su implantación. El uso de SMS para la doble autenticación es peligroso, debido a la facilidad de clonación.

1.3.3 Autenticación basada en códigos QR

Permite autenticar y autorizar el acceso a usuario haciendo uso de dispositivos móviles. Donde se recomienda la técnica "One Time Password", QR + OTP, un solo uso (como en la recuperación de contraseñas).

1.3.4 Single Sign-on (SSO)

La autenticación una sola vez en un servidor sirve para todos los recursos con los que esté relacionados. Supone un único punto de fallo, pero reducción de la superficie expuesta. Además, es más sencillo para el usuario, mejorando la experiencia de este.

Las ventajas son la usabilidad, seguridad y productividad del usuario y servidor.

2 Mecanismos de control de acceso

Son medidas que implementan y garantizan servicios en un sistema informático, particularmente en aquellos que aseguran un servicio de control de acceso.

El control de acceso implementa una política de acceso definiendo quién o qué puede tener acceso a los recursos del sistema y el tipo que se permite.

Autenticación, autorización (conceder derechos) y accounting (auditoría, registrar las acciones del usuario para permitir el no repudio) (AAA).

Podemos categorizar el control de acceso en:

- Objeto, recurso al cual se controla el acceso (registros, páginas, segmentos).
- Sujeto, entidad que potencialmente accede a los objetos.
- Derecho de acceso, describe la forma en que el sujeto podría acceder al objeto

2.1 Discretionary Access Control (DAC)

Se basa en la identidad del solicitante y reglas/condiciones de acceso. La **matriz de acceso** se la solución general para el DAC, que podría descomponerse por columnas para generar una ACL, mientras que por filas tenemos el perfil de acceso (ticket de capacidades) a los recursos del sistema.

Resulta fácil ver los permisos, revocarlos o eliminarlos, aunque las comprobaciones no son muy usables.

Una alternativa sería una tabla de acceso, por filas.

2.2 Mandatory Access Control (MAC)

Se basa en comparar etiquetas de seguridad/criticidad a los recursos (secret, top-secret, unclassified) con las entidades.

2.3 Role-based Access Control (RBAC)

Se basa en un rol del usuario y las reglas que se asocian a dicho rol. Por lo general es bastante estático. Se tendrían dos matrices, de **usuarios** con **roles** y roles con **permisos**, teniendo en cuenta la **sesión** también.

Es más flexible y granulado a la hora de gestionar condiciones de un usuario.

Se permite definir roles mutuamente exclusivos a limitar de forma estática o dinámica., cardinalidad como número máximo de roles y prerrequisitos.

- Static Separation of Duties, define roles mutuamente excluyentes.
- Dynamic Separation of Duties.

2.4 Otros mecanismos

Attribute-based Access Control (ABAC), se basa en atributos asociados con el usuario y que dependiendo del atributo se permite o no el acceso y características del usuario. El más sencillo es la mayoría de edad.

Capability-Based Access Control (CapBAC), basado en conjunto de roles (funciones) y atributos (capacidades).

Risk-Based Access Control, donde se basa en los riesgos de las acciones

$$risk = v_{info} \cdot p$$

- Valor de la información
- P probabilidad de que ocurra.

Organizational-Based Access Control (Or-BAC) mejora el uso de RBAC con sujetos, actividades y vistas sobre los recursos.

3 Protocolos criptográficos avanzados

Un protocolo criptográfico es un algoritmo distribuido para alcanzar un objetivo específico de seguridad. Los avanzados tocan temas como: Elecciones; Firma de Contratos; Transferencia inconsciente; Demostraciones de Conocimiento Nulo; Póker Mental; Lanzamiento de monedas; Canal Subliminal; Compartición de secretos

3.1 División de secretos

Un secreto se divide en varias partes que por separado no tienen demasiado significado, pero juntas permiten desvelar su secreto. El problema sería que la pérdida de una parte del mensaje

3.2 Compartición de secretos

Se basa en el concepto esquema umbral (k-n); n sombras, que con k de ellos se puede reconstruir el secreto. Para ello se eligen aleatoriamente los coeficientes de un polinomio k-l. Esto hace que las ecuaciones como sistema sea resoluble cuando se tienen k ecuaciones

3.3 Protocolo de Bit-Commitment

El problema general que este tipo de protocolos pretende resolver es el de realizar una predicción sin revelarse hasta que haya ocurrido el hecho.

Usando criptografía simétrica y hash sería posible resolver este problema, pero necesitaremos una TTP que dé constancia de que el hash de la predicción corresponde con el hash del hecho.

3.4 Lanzamiento de monedas

Supongamos que Alice desea hacer el lanzamiento de la moneda ("cara o cruz"):

- Alice debe lanzar la moneda antes de que Bob se pronuncie
- Alice no debe ser capaz de re-lanzar la moneda después del pronunciamiento de Bob
- Bob no debe saber de qué lado cayó la moneda antes de pronunciarse

Para ello se combina el protocolo de compromiso de bit con criptografía de clave pública:

- Se envían dos mensajes cifrados con clave pública de A
- B responde con uno de los mensajes cifrados con la clave pública de B
- Alice descifra el mensaje si se cumple que no importa el orden de descifrado en el algoritmo de cifrado.
- Bob descifra el mensaje y lo envía a Alice.

Bob debe asegurar que no hace trampas Alice cifrando si es necesario con la pública de A y comprobando la igualdad en los mensajes.

3.5 Póker Mental

Si se extrapola a 52 cartas de las cuales se escogen 5 entre los dos candidatos:

Alice y Bob generan, cada uno, un par clave pública/clave privada Alice: KApu , KApr Bob: KBpu , KBpr

Alice genera 52 mensajes, uno para cada carta de la baraja. Estos mensajes contienen además alguna cadena aleatoria, para verificar posteriormente su autenticidad. Alice cifra todos los mensajes con su clave pública y los envía a Bob en un orden aleatorio Alice®Bob: EApu (Mi) donde i = 1 .. 52

Bob, que no puede leer ninguno de los mensajes, elige aleatoriamente cinco de ellos; los cifra con su clave pública y se los devuelve a Alice Bob: EBpu (EApu (Mj B)) donde Mj B (j = 1..5) son las cinco cartas que Bob ha elegido

Alice, que no puede leer los mensajes que Bob le ha devuelto, los descifra con su clave privada y se los devuelve a Bob Alice: DApr (EBpu (EApu (Mj B)) Alice®Bob: EBpu (Mj B)

Bob descifra los mensajes con su clave privada para averiguar su mano Bob: DBpr (EBpu (Mj B)) = Mj B Tema 3: Esquemas, Protocolos y Mecanismos de Soporte 32 Protocolo de póker mental ⑥

De los 47 mensajes EApu (Mi) que restan de los 52 que recibió en el paso 2, Bob elige aleatoriamente cinco de ellos, EApu (Mk A), y se los envía a Alice Bob®Alice: Mk A (k = 1..5) donde Mk A (j = 1..5) son las cinco cartas de la mano de Alice

Alice descifra esos cinco mensajes y ve cuáles son las cartas que le han tocado Alice: DApu (EApu (Mk A)) = Mk A

Test

1 ¿Cuál es la ventaja adicional que nos puede proporcionar ABAC (acceso basado en atributos)?

a. Confidencialidad
b. Privacidad
c. Integridad
d. No repudio

2 ¿Cómo se consigue una Access Control List (ACL) en DAC?

a. Descomponiendo una matriz de acceso por filas (usuarios)
b. Descomponiendo una matriz de acceso por columnas (recursos)
c. A través de una Tabla de Autorización

3 ¿Cuál es la categoría de control de acceso que se basa en etiquetas de seguridad?

a. DAC
b. ABAC
c. RBAC
d. MAC

4 RESPUESTA MÚLTIPLE - ¿Cuáles son los certificados digitales contenidos dentro de un DNI-e?

a. Certificado de componente
b. Certificado de autenticación
c. Certificado de firma
d. Certificado de la CA emisora

5 ¿Cómo se comprueba la validez de un certificado digital?

a. Se aplica una función hash a los datos del certificado, y se cifran con la clave privada del emisor
b. Se aplica una función hash a los datos del certificado, y se comprueba que la firma digital coincida con ese hash
c. Se aplica una función hash a los datos del certificado, y se comprueba que ese hash coincida con el hash contenido en la firma digital
d. Se comprueba que la clave pública y la clave privada contenida en el certificado coincidan

6 Imaginemos que nos conectamos a una página web via HTTPS. Esa página se autentica mediante un certificado digital. ¿Qué debemos hacer para comprobar la validez de ese certificado?

a. Contactar con una autoridad de certificación para que ésta nos verifique el certificado
b. Comprobar que el nombre de la página web se encuentra en el campo "emisor".
c. Comprobar que el camino de certificación de la CA raíz hasta el certificado de esa página web es correcto.
d. Comprobar que la firma del emisor del certificado digital es válida

7 ¿Cuáles son los elementos básicos del control de acceso?

a. Autenticante, Autenticado, Derecho
b. Objeto, Sujeto, Entidad
c. Objeto, Sujeto, Etiqueta
d. Objeto, Sujeto, Derecho

8 ¿Cuál es la estructura estándar de certificado digital que ha sido adoptada internacionalmente?

a. Z.600
b. X.500
c. X.509
d. X.PKI.ITU

9 ¿Cuáles de los siguientes campos NO son relevantes para un documento digital que contenga la clave pública de un usuario?

a. Clave privada del usuario
b. Firma digital del emisor
c. Identidad usuario
d. Identidad emisor
e. Clave pública del usuario
f. Fecha de emisión/expiración
g. Número de serie

10 ¿Cuáles son los tokens que un usuario puede obtener en Kerberos?

a. Tokens de sesión (se obtienen una vez por sesión)
b. Tokens de servicio (se obtienen una vez por cada servicio que se desee acceder)
c. Ambas son correctas

11 ¿Cuál es el modelo PULL de distribución de claves?

a. El KDC actua como "puente" entre la entidad A y B (A contacta con el KDC, y el KDC contacta con B)
b. **La entidad A contacta primero con el KDC y antes de comunicarse con B**
c. La entidad A contacta primero con la entidad B a fin de que éste última sea la encargada de solicitar al KDC la clave correspondiente
d. Tanto las entidades A como B contactan con el KDC al mismo tiempo. Así, el KDC podrá enviarles la clave correspondiente

12 ¿Cómo se soluciona el ataque de repetición en el protocolo Needham-Schroeder?

a. **Añadiendo a los mensajes un nonce aleatorio obtenido en una comunicación inicial con Bob**
b. Añadiendo a los mensajes una marca de tiempo a los mensajes
c. Añadiendo a los mensajes un nonce aleatorio en la comunicación inicial con el KDC.
d. Añadiendo a los mensajes firmas digitales

13 ¿Cuál es la función del protocolo OCSP ?

a. **Confirmar on-line el status (revocado o no) de un certificado**
b. Confirmar on-line el status (verificado o no) de un certificado
c. Emitir certificados rápidamente gracias al uso del DNI-e
d. Proporcionar las últimas CRLs disponibles en la CA

14 ¿Cuáles son las entidades en el modelo RBAC basado en roles?

a. Usuario, rol, permiso y recurso
b. Usuario, rol, permiso y restricciones
c. **Usuario, rol, permiso y sesión**
d. Objeto, Sujeto, permiso

15 ¿Cuál es el rol principal del KDC?

a. **Actuar como servidor de confianza para el proceso de intercambio de claves**
b. Actuar como servidor de confianza, almacenando los certificados de los usuarios
c. Analizar el tráfico de la red para evitar intrusiones
d. Actuar como árbitro en la negociación de los parámetros de seguridad utilizados por los usuarios en el canal de comunicaciones

16 RESPUESTA MÚLTIPLE - ¿Con cuáles de los siguientes servicios NO está relacionado claramente el servicio de control de acceso?

a. Autenticación

b. Auditoría
c. **Integridad**
d. Autorización

17 ¿Cuáles de los siguientes servicios NO están ofrecidos por una PKI?

a. Revocación y suspensión de certificados
b. Generación de claves
c. Distribución de certificados
d. Emisión de certificados
e. **Verificación de certificados externos**
f. Certificación cruzada

18 ¿Cuáles son las principales ventajas del Single Sign-On?

a. **Usabilidad, Seguridad, Productividad**
b. Usabilidad, Robustez, Productividad
c. Usabilidad, Seguridad, Autorización
d. Usabilidad, Seguridad, Centralización

19 ¿Cuál es la principal diferencia entre una Tarjeta (Smart Card) microprocesada y una Tarjeta (Smart Card) criptográfica?

a) Ninguna diferencia, son en realidad idénticas
b) Las tarjetas criptográficas albergan datos y aplicaciones
c) **Las tarjetas criptográficas son tarjeta microprocesadas que permiten ejecutar primitivas criptográficas**
d) Las tarjetas criptográficas sólo contienen datos cifrados

Bibliografía

Tema 3 Protocolos