Examen Final 2011/2012 Pregunta 5.3

- **Autenticación Servidor:**
  - Se puede utilizar un certificado digital que contenga la clave pública del servidor y su identidad, y que esté firmado digitalmente por una tercera parte (CA) en la que confiemos. Por ejemplo, VersiSign.
  - Para garantizar más nivel de confianza, se puede mandar un desafío (autenticación basada en desafío respuesta) al servidor para comprobar que realmente tiene en su posesión la clave privada asociada a la clave pública del certificado.
  - El desafío puede ser un número aleatorio cifrado con la clave pública del servidor que está contenida en el certificado recibido. Este número se manda al servidor cifrado y se espera que lo devuelva descifrado con la clave privada. Si coincide con el valor enviado nos indicaría que el servidor tiene en su propiedad la clave privada correspondiente.

Examen Final 2011/2012 Pregunta 5.3

- **Autenticación Cliente:**
  - La autenticación en el lado del cliente puede estar basada en verificar algo que el usuario sabe, por ejemplo, una contraseña. Dicha contraseña se podría fijar en la fase de registro enviándola cifrada al servidor con su clave pública. En posteriores autenticaciones se enviará una función hash + nº aleatorio al servidor para que compruebe su validez.

  - Otra opción sería utilizar un valor que evitase al usuario tener que introducir todo el rato la contraseña. Se podrían utilizar algo que el usuario tiene. Un ejemplo podría ser el IMEI del teléfono móvil o la dirección MAC de la interfaz wireless del teléfono. Se podría combinar con el método anterior para mayor robustez.

  - Una última posibilidad podría ser la utilización de rasgos biométricos para la autenticación, extraídos de una foto del usuario. Se podrían enviar cifrados con la clave pública del servidor.

Examen Final 2011/2012 Pregunta 5.3

- **Confidencialidad e Integridad:**
  - Para garantizar la confidencialidad de la información ésta debería transmitirse cifrada. Frente a los métodos de cifrado asimétrico preferiríamos los métodos simétricos por su mayor eficiencia. Habría que usar algoritmos robustos con un número muy grande de claves, TDES o AES, y evitar DES.
  - Para resolver el problema del intercambio de la clave se podría usar cifrado asimétrico, mandando la clave de cifrado simétrico cifrada con la clave pública del servidor. Otra opción sería usar el método de Diffie-Hellman para acordar una clave entre ambos extremos.
  - Para garantizar la integridad de los mensajes se podría calcular y enviar junto con el mensaje una función de resumen que dependiese del mensaje y de una clave especial fijada del modo anterior.
  - Todo esto se podría llevar a cabo de forma transparente usando TLS.

Examen Final 2011/2012 Pregunta 5.3

- **Diagrama Cliente Servidor:**
  - El diagrama muestra la arquitectura sugerida, la cual incorpora un cortafuegos como elemento defensivo. Todo el tráfico no relacionado con la aplicación (no originado o no con destino al puerto 443) sería filtrado.
  - En el cortafuegos registraría accesos no permitidos y un sistema de monitorización de incidencias informaría de alarmas al sobre-pasarse un cierto umbral de alerta.