Respuesta Ejercicio 2

Para permitir la captura y transmisión de información sensible de forma segura entre el cliente de la aplicación (App) y el servicio de autorización (Authorizer API) podemos hacer uso de las firmas digitales y la criptografía asimétrica, que no es más que un sistema que utiliza dos claves: una pública y otra privada. La clave pública se utiliza para cifrar mensajes y la clave privada para descifrarlos. Esto garantiza la confidencialidad del mensaje y la autenticidad del remitente. Además, este sistema evita el problema del intercambio de claves de los sistemas de cifrado simétricos.

A continuación se describe un método propuesto:

1. Generación de claves:
   - El servicio de autorización generará un par de claves asimétricas: una clave pública y una clave privada.
   - La clave privada se mantendrá en el servicio de autorización de forma segura y no se compartirá.
   - La clave pública se distribuirá a la aplicación y se utilizará para cifrar los datos sensibles.

2. Captura y cifrado de datos:
   - La aplicación cliente captura la información sensible del usuario.
   - Utilizando la clave pública del servicio de autorización, la aplicación cliente cifra los datos sensibles.
   - Solo el servicio de autorización, con su clave privada correspondiente, podrá descifrar los datos.

3. Firma digital:
   - La aplicación cliente genera una firma digital de los datos sensibles utilizando su propia clave privada.
   - La firma digital garantiza la integridad de los datos y verifica que no hayan sido modificados durante la transmisión.

4. Transmisión de datos:
   - La aplicación cliente envía los datos cifrados y la firma digital a través de la API APP hacia el servicio de autorización.
   - Los datos cifrados y la firma digital se transmiten como carga útil en la solicitud de la API APP.

5. Recepción y verificación de datos:
   - El servicio de autorización recibe los datos cifrados y la firma digital desde la API APP.
   - Utilizando su clave privada, el servicio de autorización descifra los datos sensibles.
   - El servicio de autorización verifica la firma digital utilizando la clave pública de la aplicación. Si la firma es válida, garantiza que los datos no se han modificado durante la transmisión.

Con este enfoque, los datos sensibles se cifran utilizando la clave pública del servicio de autorización, lo que garantiza que solo el servicio de autorización pueda descifrarlos con su clave privada correspondiente. Además, la firma digital garantiza que los datos no hayan sido modificados durante la transmisión.