CONTENIDO

LISTA DE FIGURAS

ANEXO E
ANÁLISIS Y DISEÑO DEL PROTOTIPO

1. ANÁLISIS

El prototipo mediante el cual se validó la plataforma “P3SIM” consta de dos partes: una parte cliente (un MIDlet J2ME) y una parte servidor que es manejada por el Proveedor del servicio.

Para mayor información acerca del diseño de P3SIM remitirse al Anexo D. El prototipo consiste en la compra y venta de artículos sobre Internet desde un dispositivo móvil (m-commerce).

1.1. Descripción del prototipo

Un usuario puede seleccionar en el MIDlet las siguientes funciones:

1. Inicialmente el usuario se suscribe al servicio mediante un menú proporcionado en el MIDlet. La suscripción es un proceso que se realiza una sola vez y en ella el usuario escribe sólo sus datos personales (no se incluye información critica tal como cuentas bancarias). De esta forma el cliente le envía al servidor los parámetros SIM del usuario (en este caso el IMSI y el ICCID).

2. Luego el usuario puede acceder al servicio con sólo escoger la opción “Ingresar”. Por debajo el MIDlet obtiene una clave simétrica DES que se crea con base en el IMSI del usuario, con esta clave se cifra el IMSI y luego se envía junto con el ICCID del usuario. El proveedor de servicio tiene tanto el IMSI como el ICCID de manera que puede generar la misma clave DES y con ella descifrar la información que le llego, el ICCID actúa como el login. Si la **información no ha sido alterada en el camino**, el Proveedor de servicio debe obtener el IMSI que tiene almacenado en su base de datos, con lo cual quedará autenticado el usuario y se le permitirá el acceso al servicio.

3. Una vez el usuario accede al servicio, para que el usuario obtenga una máxima seguridad es recomendable cambiar las claves. Con solo presionar “cambiar claves”, el MIDlet actualizará todas las claves simétricas, y si no existe, también la clave pública del proveedor de servicio. Para lograr esto, el Proveedor de servicio le envía al MIDlet las claves en un formato cifrado, de manera que **el MIDlet las descifre y luego almacene**.

4. Cuando el usuario va a **buscar un producto**, el puede comprobar que efectivamente los datos del producto son los originales (Integridad de la información) y que el vendedor es realmente quien dice ser. Esto lo logra el MIDlet mediante **la verificación de la firma digital** que acompaña a los datos de dicho producto.

5. Para pagar un producto el usuario debe escribir los datos de su tarjeta de crédito. Como esta información es tan crítica, estos datos se **cifran asimétricamente** con la clave RSA pública del proveedor de servicio, de manera tal que la única forma de obtener dicha información sea **descifrándola con la clave privada** del proveedor de servicio del lado del servidor.

6. Finalmente para ofrecer un producto, el usuario debe escribir los datos del producto (**pueden ser una gran cantidad de datos**). Por debajo el MIDlet **generará una firma digital** de dichos datos (es mas **eficiente** obtener una firma digital que cifrar todos los datos) y le enviará al proveedor de servicio tanto los datos del producto como su firma. Adicionalmente se da la opción de enviar una foto del producto. Al verificar la firma digital que le llegó, el proveedor de servicio podrá comprobar la integridad de los datos del producto y validar quien los emitió.

1.2. Diagrama de casos de uso

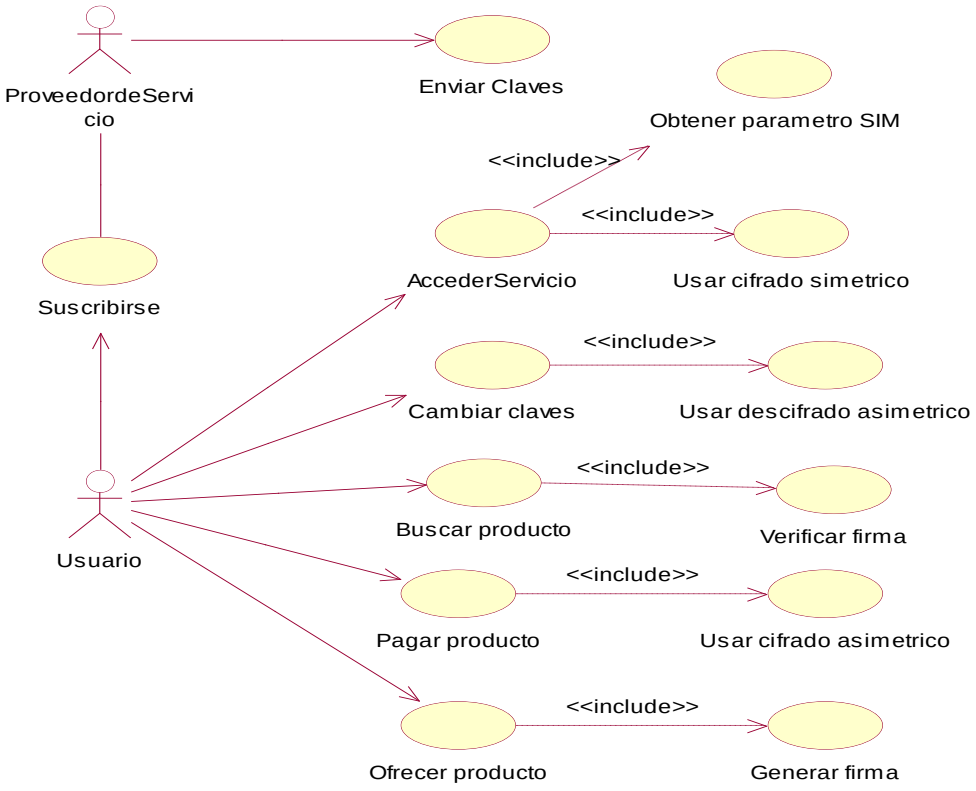

Figura 1-1. Diagrama de casos de uso del prototipo

1.3. Descripción de los casos de uso

Para ver la descripción de los casos de uso: Obtener parámetros SIM, Usar cifrado simétrico, Usar descifrado asimétrico, Verificar firma, Usar cifrado asimétrico y Generar firma, remitirse al Anexo D.

Información General	
Caso de uso:	**Suscribirse**
Actores:	Usuario
Propósito:	Permitirle al proveedor de servicio conocer los parámetros SIM del usuario.
Resumen:	El Usuario digita su nombre y presiona la opción “suscribirse”. El MIDlet adicionalmente al nombre, envía los parámetros SIM IMSI y el ICCID al servidor.
Tipo:	Primario.
Referencias cruzadas:	No hay.
Precondiciones	
- El SECApplet debe estar instalado en la tarjeta SIM.	

Flujo Principal
− El usuario ingresa a la opción suscribirse del MIDlet.
− El MIDlet le muestra al usuario un espacio para que se digite el nombre.
− El usuario presiona la opción “suscribirse”
− El MIDlet haciendo uso de P3SIM obtiene el ICCID y el IMSI del usuario.
− El MIDlet envía al servidor el nombre, el ICCID y el IMSI del usuario.
− El servidor retorna un mensaje informando del éxito en la suscripción del usuario.
− El MIDlet le muestra al usuario el mensaje de éxito.

Flujos de Excepción
E1: Parámetros SIM no accesibles.
− Por alguna razón no se pudo obtener el ICCID o el IMSI del usuario.
− Se le muestra al usuario el mensaje de fracaso en la suscripción.

Información General	
Caso de uso:	**Acceder servicio**
Actores:	Usuario
Propósito:	Permitirle al usuario acceder al servicio.
Resumen:	El MIDlet envía el ICCID y el IMSI cifrado del usuario al servidor.
Tipo:	Primario.
Referencias cruzadas:	No hay.
Precondiciones	

- El Usuario tiene que estar registrado (suscribirse previamente) ante el proveedor de servicio.
- El SECApplet debe estar instalado en la tarjeta SIM.

Flujo Principal

- El usuario selecciona la opción “ingresar”.
- El MDlet obtiene una clave DES (conocida por el proveedor del servicio) y cifra el IMSI del usuario, luego lo envía junto al ICCID.
- El servidor valida estos datos y le envía al usuario la respuesta OK.
- El MIDlet le permite al usuario acceder a todas las opciones del prototipo: comprar producto, …

Flujos de Excepción

E1: Parámetros SIM o clave DES no accesible.

- Se le muestra al usuario el mensaje de fracaso en el ingreso.

Información General

Caso de uso:	**Cambiar claves**
Actores:	Usuario
Propósito:	Permitirle al usuario cambiar sus claves.
Resumen:	El Servidor le envía las nuevas claves al MIDlet y luego se almacenan en la tarjeta SIM.
Tipo:	Primario.
Referencias cruzadas:	Enviar clave.

Precondiciones

- El Usuario tiene que estar registrado (suscribirse previamente) ante el proveedor de servicio.
- El SECApplet debe estar instalado en la tarjeta SIM.

Flujo Principal

- El usuario selecciona la opción “cambiar claves”.
- El servidor le envía al MIDlet las nuevas claves cifradas con la clave pública del usuario.
- El MIDlet descifra dichas claves con la clave privada del usuario.
- El MIDlet almacena las nuevas claves.
- El MIDlet le muestra al usuario el mensaje “claves cambiadas exitosamente”

Flujos de Excepción

E1: Error criptográfico.

- Si en el recorrido fue alterada la información enviada del servidor al cliente, se produce una excepción de seguridad.
- Se le muestra al usuario el mensaje “no se pudieron cambiar las claves”.

Información General	
Caso de uso:	**Enviar claves**
Actores:	Proveedor de servicio
Propósito:	Permitirle al usuario cambiar las claves.
Resumen:	El servidor le envía al usuario una clave nueva, esta clave es enviada en un formato cifrado.
Tipo:	Primario.
Referencias cruzadas:	No hay.

Precondiciones

- El Usuario tiene que estar registrado (suscribirse previamente) ante el proveedor de servicio.
- El SECApplet debe estar instalado en la tarjeta SIM.

Flujo Principal

- El usuario selecciona la opción “cambiar claves”.
- El proveedor de servicio genera una nueva clave y luego la cifra con la clave pública del usuario. Se envía al cliente la nueva clave cifrada.
- El MDlet recibe la información y la descifra con la clave privada del usuario.
- El MIDlet almacena la nueva clave en la tarjeta SIM.
- El MIDlet le muestra al usuario el mensaje de éxito

Flujos de Excepción

E1: Error criptográfico.

- Si en el recorrido fue alterada la información enviada del servidor al cliente, se produce una excepción de seguridad.
- Se le muestra al usuario el mensaje “error en el cambio de claves”.

Información General	
Caso de uso:	**Buscar producto**
Actores:	Usuario
Propósito:	Permitirle al usuario buscar un producto.
Resumen:	El servidor le envía al usuario la descripción de un producto junto con su firma digital.
Tipo:	Primario.
Referencias cruzadas:	No hay.

Precondiciones

- El Usuario tiene que estar registrado (suscribirse previamente) ante el proveedor de servicio.
- El SECApplet debe estar instalado en la tarjeta SIM.

Flujo Principal

- El usuario entra a la opción “Buscar producto”.

- El servidor le envía al cliente la lista de los productos disponibles.
- El usuario selecciona algún producto disponible.
- El servidor le envía al cliente la descripción de un producto junto con su firma digital
- El MIDlet le muestra al usuario la información del producto, siempre y cuando la firma obtenida sea válida.

Flujos de Excepción

E1: Error criptográfico.

- Si en el recorrido fue alterada la información enviada del servidor al cliente, se produce una excepción de seguridad.
- Se le muestra al usuario el mensaje “no se puede observar la información del producto”.

Información General	
Caso de uso:	**Pagar producto**
Actores:	Usuario
Propósito:	Permitirle al usuario pagar un producto.
Resumen:	El usuario le envía al servidor el número de su cuenta bancaria cifrada asimétricamente.
Tipo:	Primario.
Referencias cruzadas:	No hay.

Precondiciones

- El Usuario tiene que estar registrado (suscribirse previamente) ante el proveedor de servicio.
- El SECApplet debe estar instalado en la tarjeta SIM.

Flujo Principal

- El usuario entra a la opción “pagar producto”.
- El usuario digita su número de cuenta bancaria y selecciona la opción “pagar”.
- El MIDlet cifra el número de cuenta bancaria con la clave pública del proveedor de servicio.
- El MIDlet le envía el número de cuenta bancaria cifrado.
- El Servidor descifra esta información con la clave privada del proveedor de servicio. Si este proceso es exitoso se le envía al cliente el mensaje de éxito.
- El MIDlet le muestra al usuario el mensaje “producto pagado”

Flujos de Excepción

E1: Error criptográfico.

- Si en el recorrido fue alterada la información enviada del cliente al servidor, se produce una excepción de seguridad.
- Se le muestra al usuario el mensaje “no se puede pagar el producto”.

Información General	
Caso de uso:	**Ofrecer producto**
Actores:	Usuario
Propósito:	Permitirle al usuario ofrecer un producto en el servidor.
Resumen:	El usuario le envía al servidor la descripción del producto y la firma digital de dicha descripción.
Tipo:	Primario.
Referencias cruzadas:	No hay.
Precondiciones	
- El Usuario tiene que estar registrado (suscribirse previamente) ante el proveedor de servicio. - El SECApplet debe estar instalado en la tarjeta SIM.	

Flujo Principal
− El usuario entra a la opción “ofrecer producto”. − El usuario digita la descripción del producto. − El MIDlet genera la firma digital de la descripción del producto. − El MIDlet le envía al servidor la descripción del producto y la firma digital. − El servidor verifica la firma digital. Si la firma es válida, se le envía al cliente el mensaje de éxito. − El MIDlet le muestra al usuario el mensaje “producto ofrecido”

Flujos de Excepción
E1: Error criptográfico. − Si en el recorrido fue alterada la información enviada del cliente al servidor, se produce una excepción de seguridad. − Se le muestra al usuario el mensaje “no se puede ofrecer el producto”.

2. DISEÑO

El diseño del prototipo se basa en la arquitectura MVC (Modelo-Vista-Control).

2.1. Diagramas de secuencia

Se realizó un diagrama de secuencia para cada caso de uso.

Caso de uso: Suscribirse

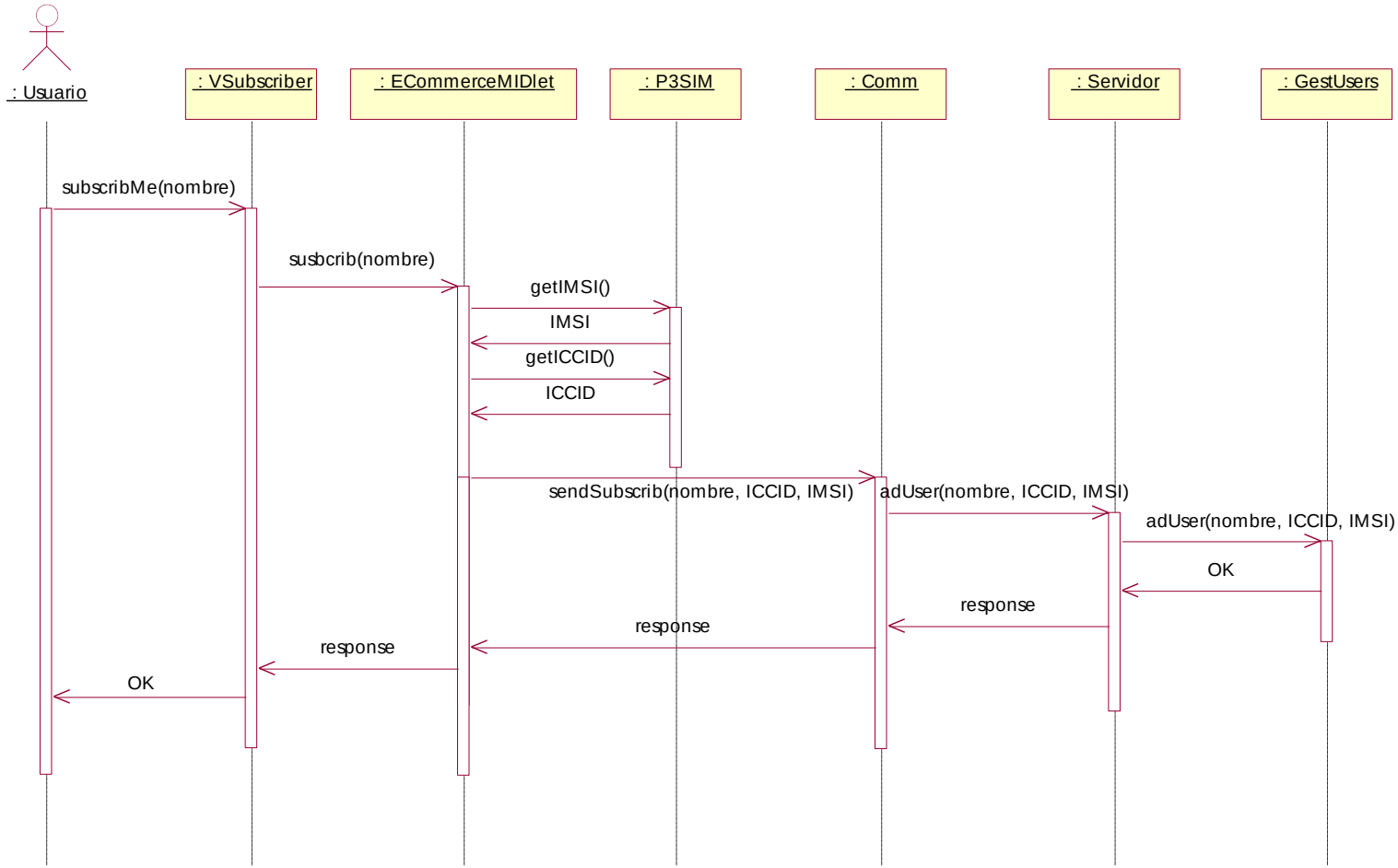

Figura 2-1. Diagrama de secuencia para Suscribirse

Caso de uso: Acceder servicio

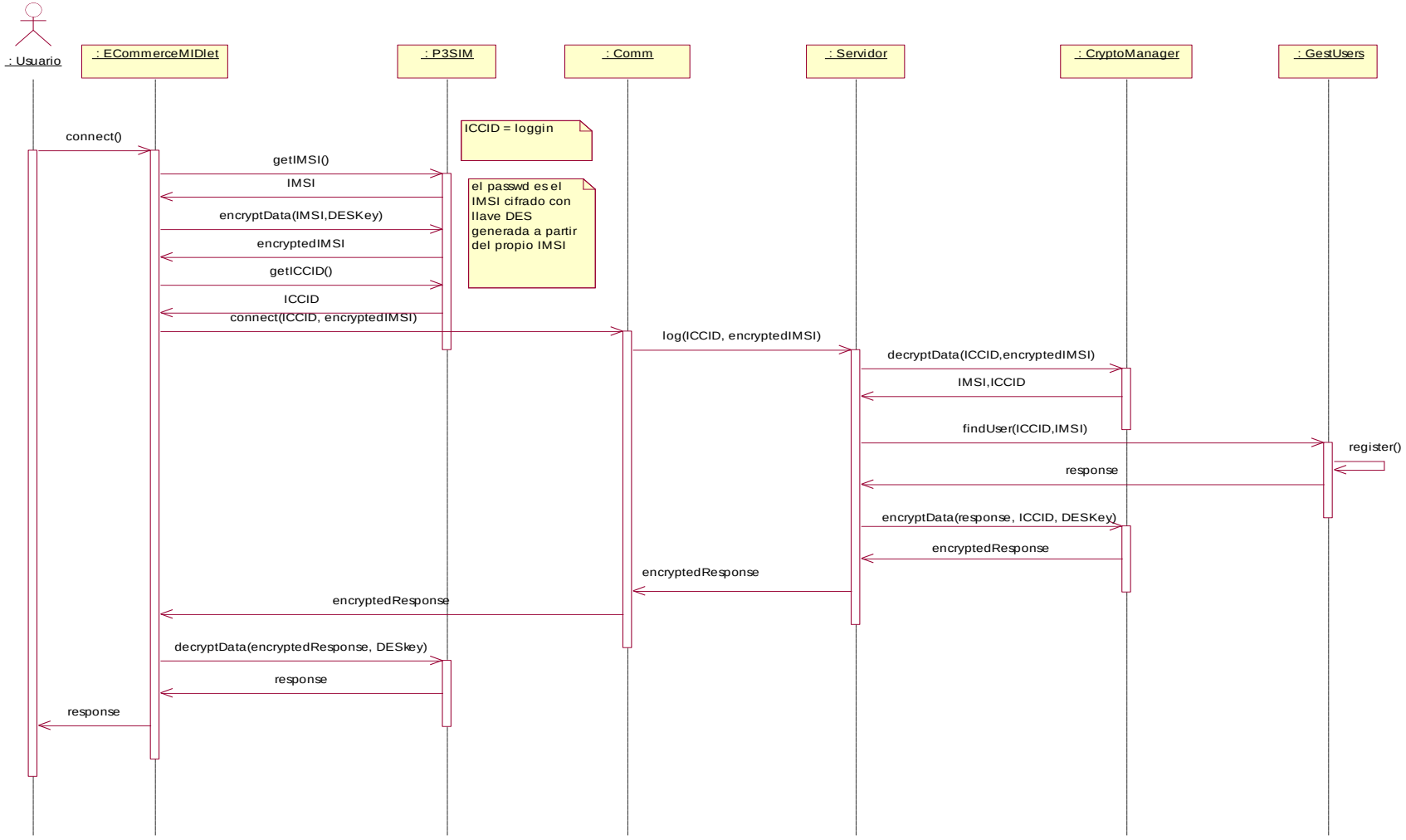

Figura 2-2. Diagrama de secuencia para Acceder servicio

Caso de uso: Buscar producto

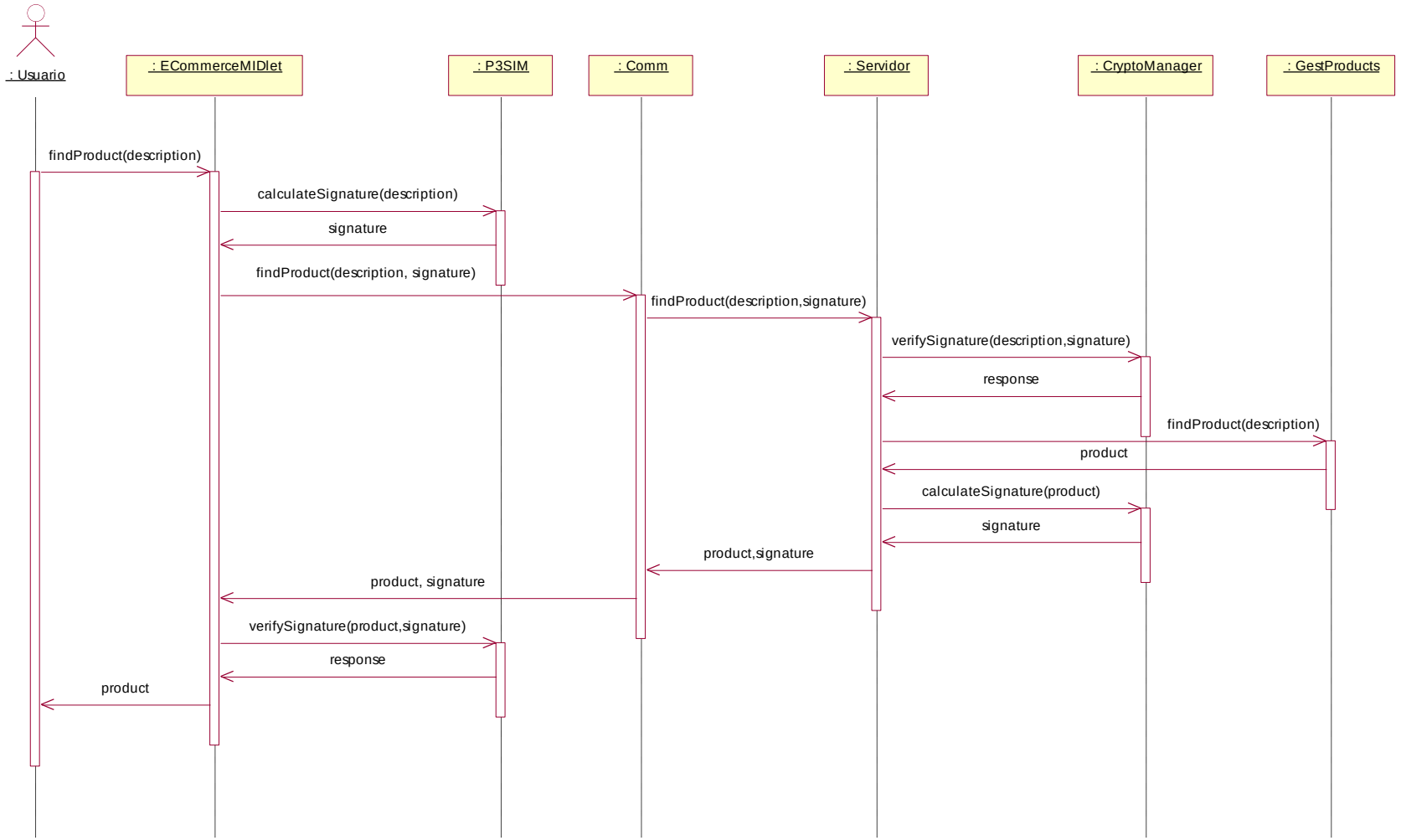

Figura 2-3. Diagrama de secuencia para Buscar producto

Casos de uso: Cambiar claves

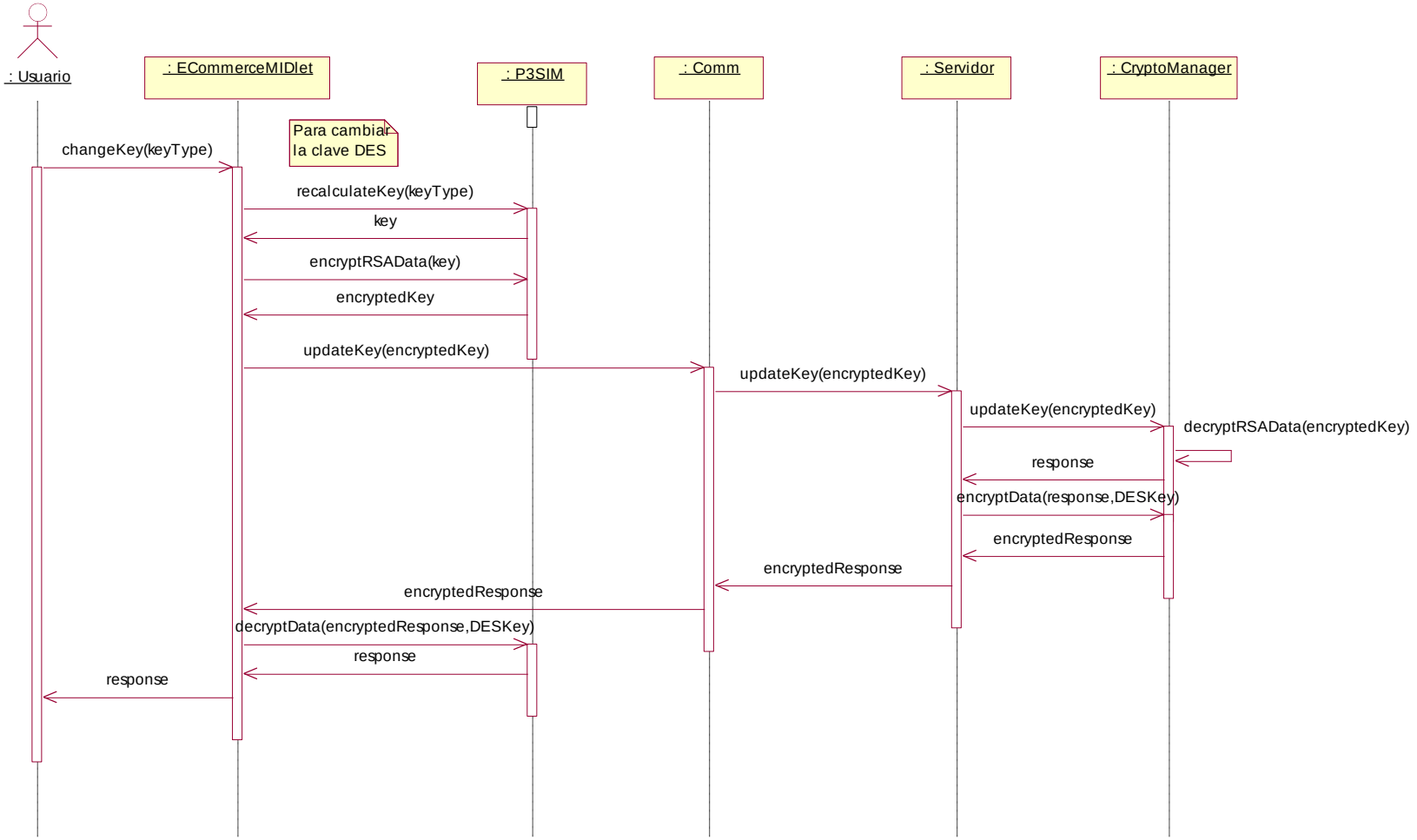

Figura 2-4. Diagrama de secuencia para Cambiar claves

Caso de uso: Enviar claves

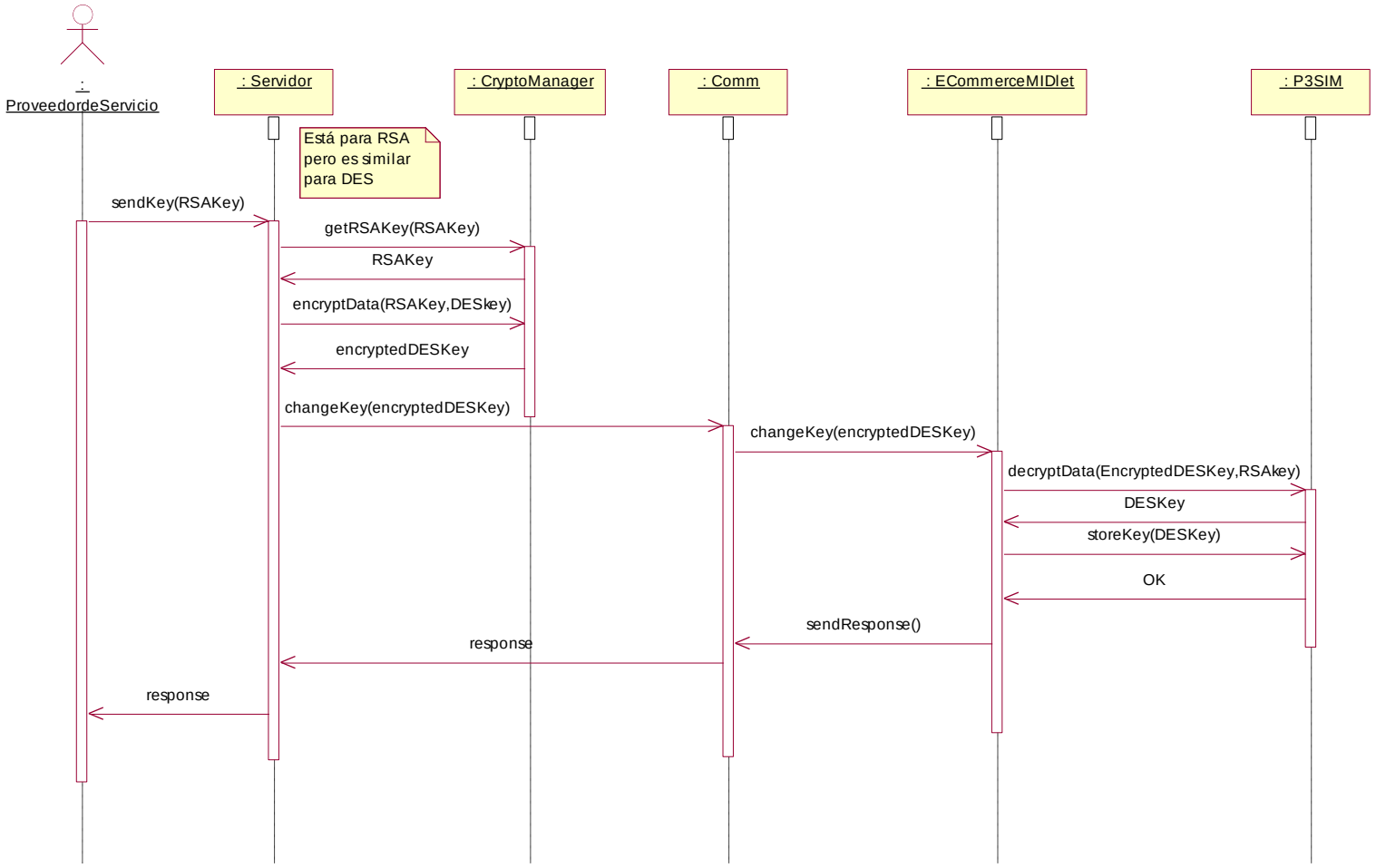

Figura 2-5. Diagrama de secuencia para Enviar claves

Caso de uso: Ofrecer producto

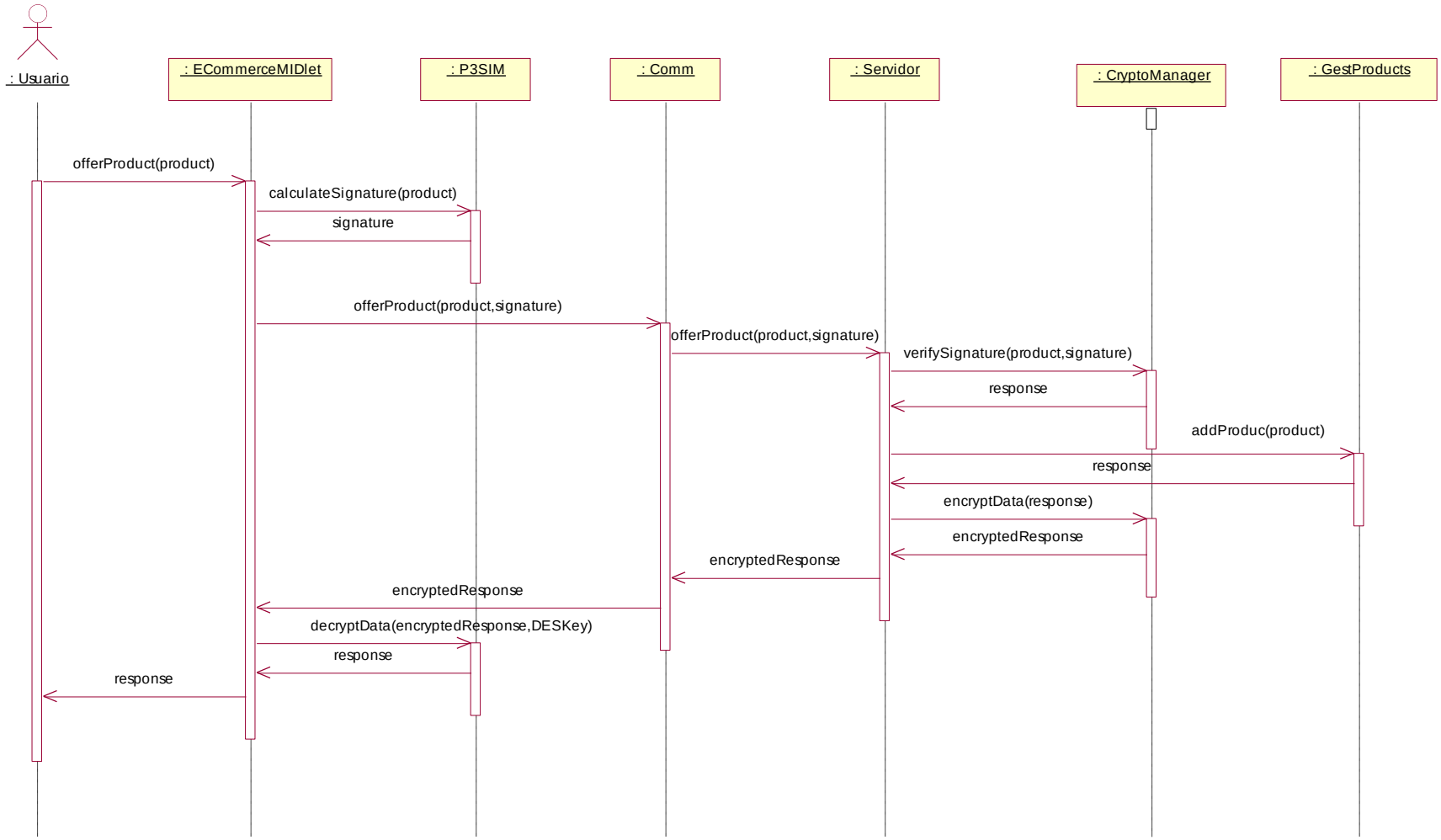

Figura 2-6. Diagrama de secuencia para Ofrecer producto

Caso de uso: Pagar producto

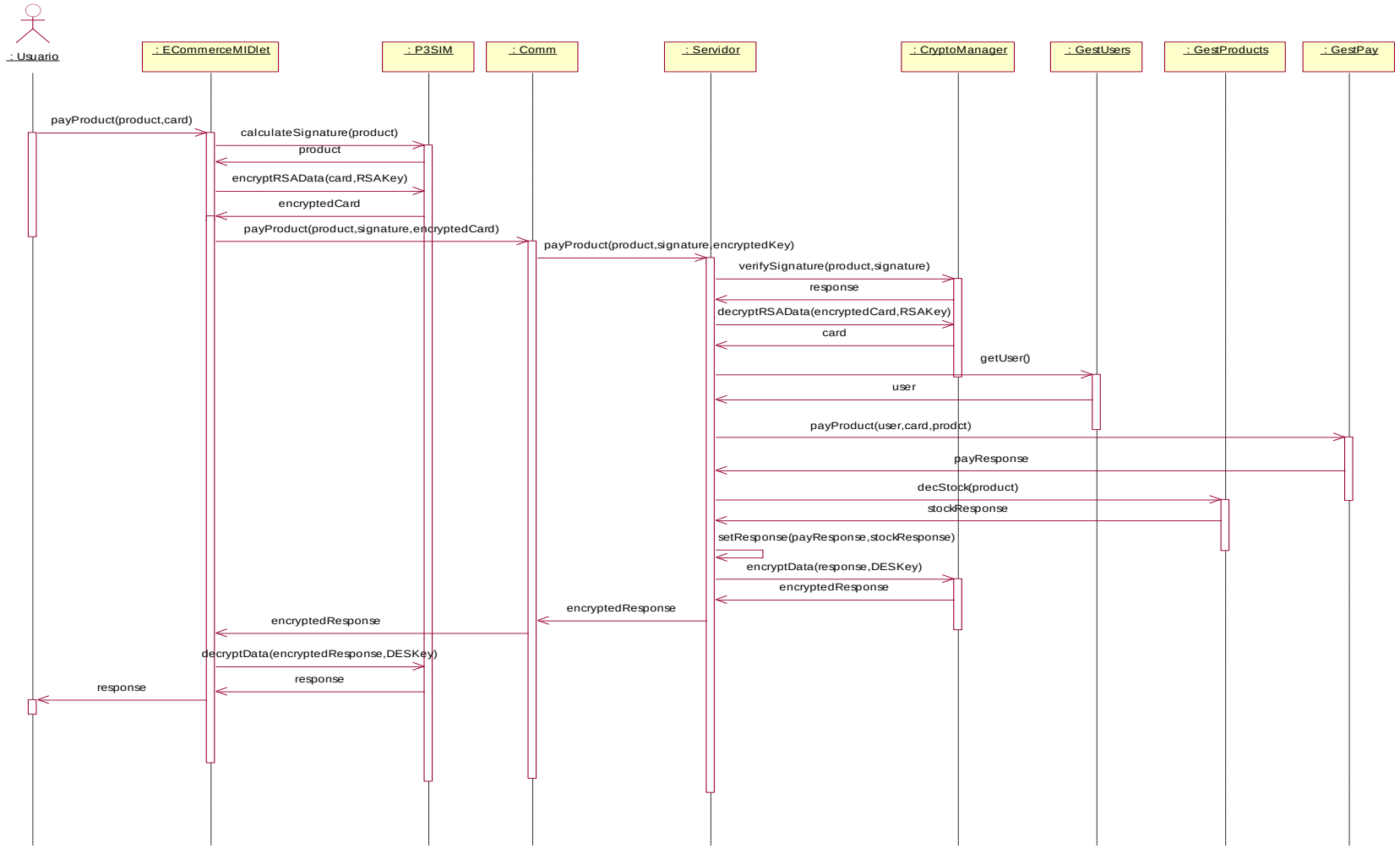

Figura 2-7. Diagrama de secuencia para Pagar producto

2.2. Diagrama de clases

La arquitectura del sistema como se mencionó anteriormente está compuesta de dos partes: el cliente (figura 2-8) y el servidor (figura 2-9).

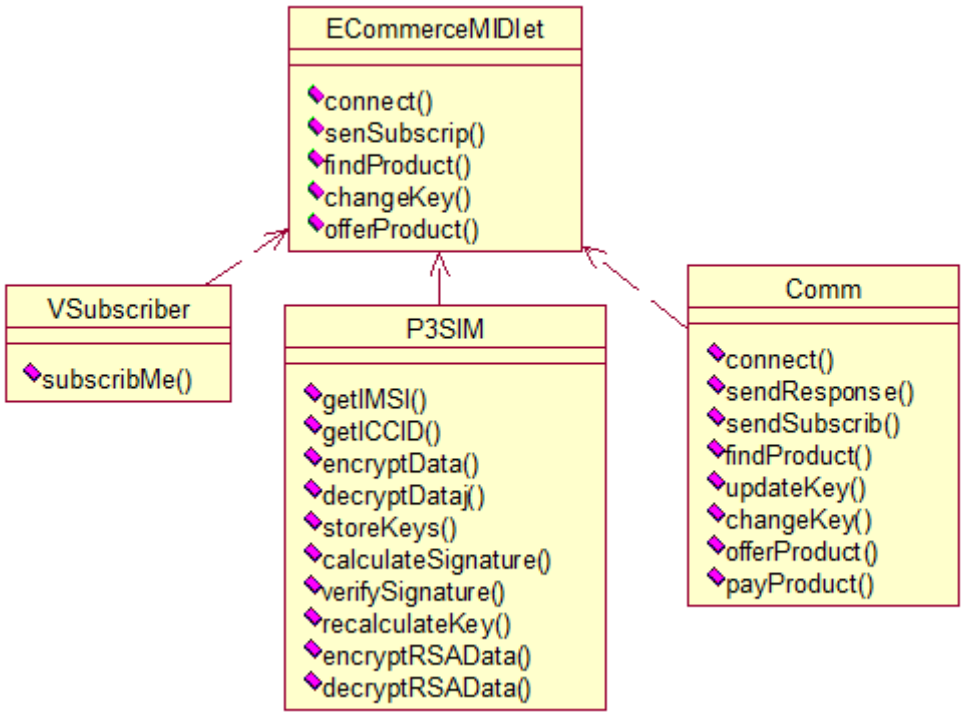

Figura 2-8. Diagrama de clases del cliente del prototipo

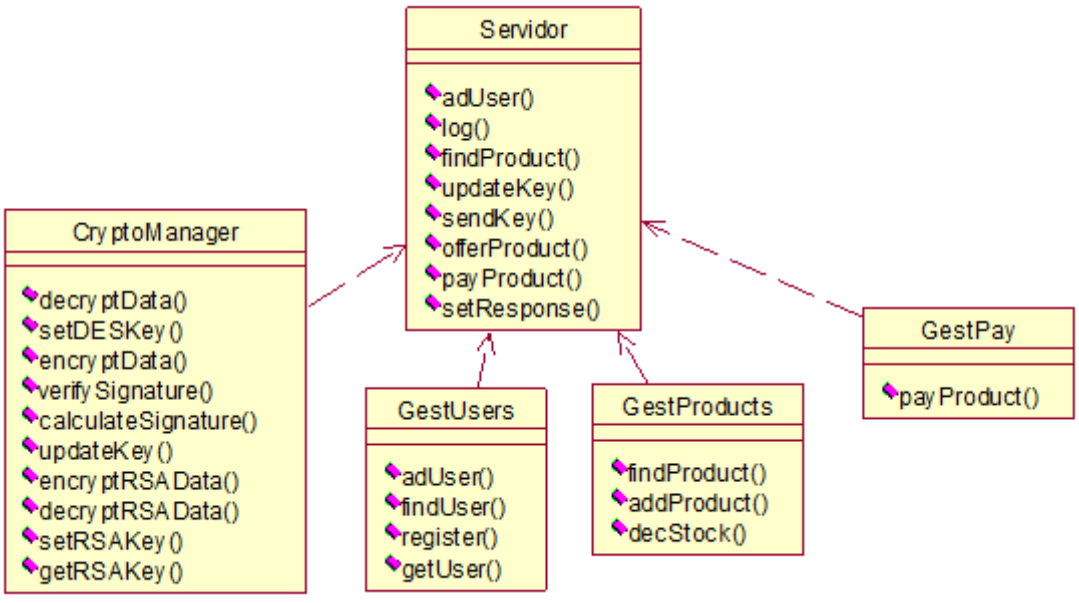

Figura 2-9. Diagrama de clases del servidor del prototipo

2.3. Diagrama de despliegue

El diagrama de despliegue se muestra en la figura 2-10. En el servidor se manejan dos conceptos:

- Gestión de la seguridad: lo cual es efectuado por las clases CryptoManager y GestUsers.
- Gestión de comercio: lo cual es realizado por las clases GestProducts y GestPay.

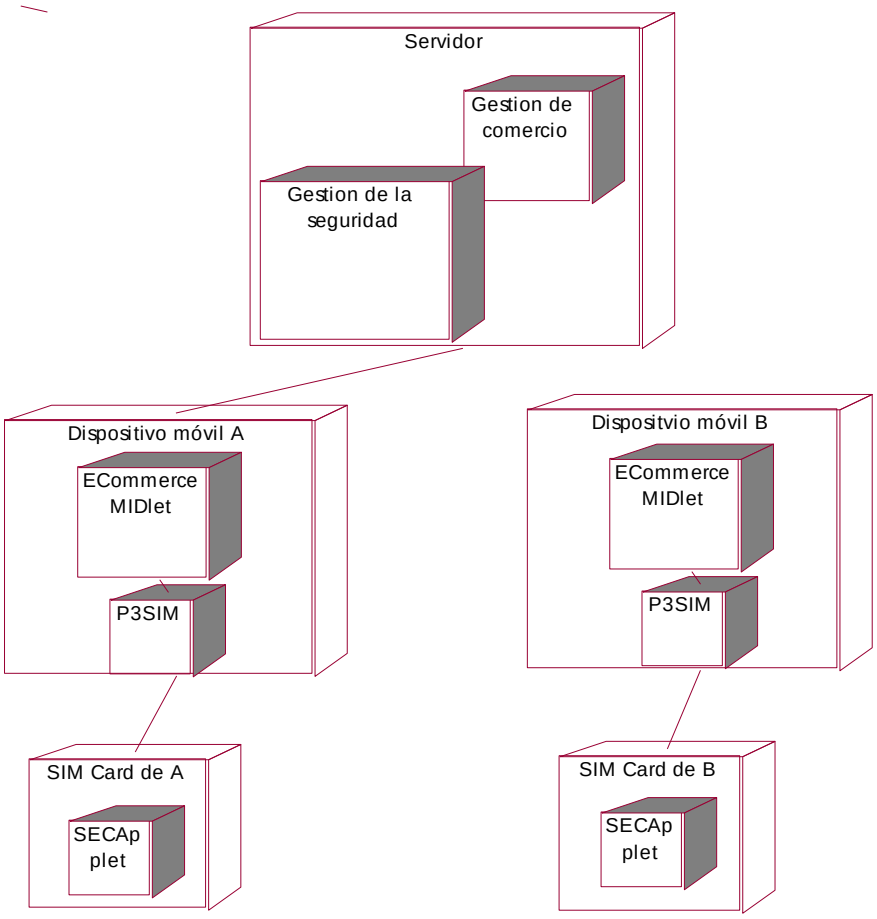

Figura 2-10. Diagrama de despliegue del prototipo