CONTENIDO

LISTA DE FIGURAS

ANEXO D
ANÁLISIS Y DISEÑO DE LA PLATAFORMA

1. ANÁLISIS

Inicialmente se había concebido una plataforma que permitiera el acceso seguro a servicios móviles basado en parámetros SIM, pero luego de un estudio mucho mas profundo de tecnologías como Java Card y SATSA (*Security And Trust Services API*) se llegó a la conclusión de que se podía construir una plataforma que permitiera algo mas que el acceso seguro a un servicio.

Lo que finalmente se concibe es una plataforma que permite:

- Acceso seguro a servicios móviles basado en parámetros SIM.
- Cifrar o descifrar información tanto con algoritmos simétricos como con asimétricos.
- Gestionar (fijar, recalcular u obtener) de forma segura en la SIM claves simétricas y asimétricas.
- Manejo de funciones Hash, con el objetivo de generar y verificar firmas digitales.

Se ha denominado a la plataforma como “P3SIM” acrónimo de “Plataforma de Seguridad para Servicios móviles basada en SIM”. La etapa de análisis descrita en este capítulo se centra en los casos de uso.

1.1. Diagrama de casos de uso

P3SIM les permitirá a los proveedores de servicios desarrollar aplicaciones seguras para dispositivos móviles.

Teniendo en cuenta lo planteado anteriormente, en la figura 1-1 se tiene el diagrama de casos de uso de la plataforma.

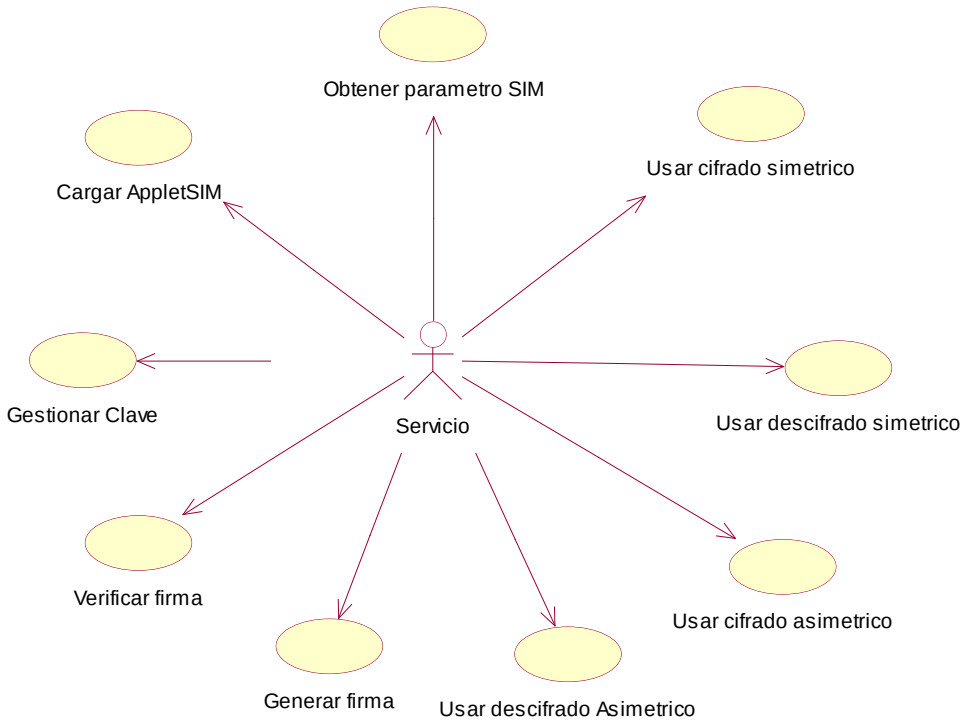

Figura 1-1. Diagrama de casos de uso de la plataforma

El actor denominado “Servicio” corresponde al servicio o aplicación(es) que estará(n) alojada(s) en el dispositivo móvil y que haciendo uso de la plataforma brindará el nivel de seguridad apropiado para cada usuario.

1.2. Descripción de los casos de uso

Información General	
Caso de uso:	**Cargar AppletSIM**
Actores:	Servicio
Propósito:	Permitir que el servicio instale un Applet en la tarjeta SIM.
Resumen:	El servicio le pasa a la plataforma archivo que representa un Applet el cual será cargado en la SIM. Una vez se carga el applet, se procede a inicializarlo.
Tipo:	Primario.
Referencias cruzadas:	No hay.
Precondiciones	
- El archivo contiene APDUs que deben cumplir con el estándar GSM 03.48.	

Flujo Principal
– El servicio le indica a la plataforma cual es el archivo que contiene los APDUs para que

posteriormente la plataforma le envíe las APDUs a la SIM.
- Luego la plataforma trata de seleccionar el Applet.
- Si la selección es exitosa, entonces la plataforma le envía al servicio el mensaje de instalación exitosa.

Flujos de Excepción
E1: El Applet no pudo ser seleccionado.
- La plataforma tuvo algún problema al cargar al Applet en la SIM y por eso el applet no puede ser seleccionado. - La plataforma le envía al servicio el respectivo mensaje de error.

Información General	
Caso de uso:	**Obtener parámetro SIM**
Actores:	Servicio
Propósito:	Permitir que el servicio obtenga algún parámetro SIM.
Resumen:	La plataforma le envía al Applet en la SIM un command APDU que sirve para obtener el parámetro que especificó el servicio, luego la SIM le retorna el parámetro SIM a la plataforma.
Tipo:	Primario.
Referencias cruzadas:	No hay.
Precondiciones	
- El applet debe estar instalado en la tarjeta SIM.	

Flujo Principal
- El servicio le especifica la plataforma que parámetro SIM quiere obtener. - La plataforma le pide el parámetro específico al Applet en la SIM - La SIM le retorna el parámetro a la plataforma. - La plataforma le envía el parámetro al servicio.

Flujos de Excepción
E1: El parámetro no existe.
- Debido a que algunos parámetros de la SIM puede estar opcionalmente en las tarjetas reales, se puede presentar el caso se que el parámetro no exista. - La plataforma le envía al servicio el respectivo mensaje de error.

Información General	
Caso de uso:	**Gestionar clave**
Actores:	Servicio
Propósito:	Permitir que el servicio almacene, actualice u obtenga una clave en la tarjeta SIM.
Resumen:	El servicio puede crear una clave, obtenerla, actualizarla o almacenarla. Todo ello la plataforma lo realiza sobre la tarjeta SIM.
Tipo:	Primario.
Referencias cruzadas:	No hay.
Precondiciones	
- El applet debe estar instalado en la tarjeta SIM.	

Flujo Principal

- El servicio especifica lo que quiere hacer: generar, obtener o almacenar una clave. Subflujos S1, S2 ó S3.
- Se le informa al servicio del éxito o fracaso de la operación.

Subflujos

S1: Generar una clave

- La plataforma le ordena a la tarjeta SIM que genere el tipo de clave que el servicio especifica.
- Luego esa clave se almacena en la SIM.

S2: Obtener una clave

- El servicio le informa a la plataforma qué clave en particular quiere obtener.
- La plataforma obtiene la clave desde la tarjeta SIM y se la retorna al servicio.

S3: Almacenar una clave.

- El servicio le envía a la plataforma una nueva clave, para que sea almacenada en la tarjeta SIM. El servicio debe informar las características de la clave que ha enviado: si es simétrica o asimétrica (publica o privada), el algoritmo de cifrado para el que es utilizada.

Flujos de Excepción

E1: La Clave no es una clave válida.

- La plataforma no soporta el tipo de clave especificada por el servicio.
- No se almacena ni se actualiza ninguna clave

Información General

Caso de uso:	**Verificar firma**
Actores:	Servicio
Propósito:	Garantizar la integridad de la información y el no repudio.
Resumen:	El servicio obtiene una información con su respectiva firma digital. Este caso de uso permite verificar la validez de dicha firma digital con respecto a la información recibida.
Tipo:	Primario.
Referencias cruzadas:	- Gestionar claves - Usar descifrado asimétrico

Precondiciones

- El applet debe estar instalado en la tarjeta SIM.

Flujo Principal

- El servicio le pasa a la plataforma tres parámetros: la información recibida, la firma digital y la clave pública de la entidad que envió la información.
- La plataforma descifra con la clave pública la firma digital, obteniendo un hash.
- Luego calcula el hash de la información recibida.
- Se comparan los dos hash.
- Si los hash son iguales, se le informa al servicio de la validez de la firma. Si no son iguales se le informa lo contrario.

Flujos de Excepción

E1: No se puede descifrar la firma digital.

- La plataforma lanza una excepción debido a tres posibilidades: la firma no es válida, la clave

pública no es válida, el algoritmo con que se obtuvo la firma no es soportado.

Información General	
Caso de uso:	**Generar firma**
Actores:	Servicio
Propósito:	Este caso de uso permite calcular la firma digital de cualquier información.
Resumen:	El servicio debe especificar los datos de entrada (información) y el tipo de algoritmo usado para obtener la firma. Internamente la plataforma también hará uso de las claves asimétricas del usuario.
Tipo:	Primario.
Referencias cruzadas:	Gestionar claves.
Precondiciones	
- El applet debe estar instalado en la tarjeta SIM. - Deben estar almacenadas la clave pública y privada del usuario.	

Flujo Principal
− La plataforma le calcula el hash a la información proporcionada por el servicio. − La plataforma le envía a la SIM el hash para que la tarjeta lo cifre con la clave privada del usuario. La SIM retorna a la plataforma el hash cifrado. − La plataforma obtiene la clave pública del usuario, la cual está almacenada en la SIM. − La plataforma le retorna al servicio el hash cifrado y la clave pública del usuario.

Flujos de Excepción
E1: El algoritmo para generar la firma no está soportado. − Se le informa al servicio, del fracaso al generar la firma con dicho algoritmo.

Información General	
Caso de uso:	**Usar descifrado asimétrico**
Actores:	Servicio
Propósito:	Permitirle conocer al servicio si la información que le llegó no ha sido modificada. Dependiendo de si la cifraron con una llave pública o una privada permite garantizar que el usuario es el destino real o que la entidad que lo envió es realmente quien dice ser.
Resumen:	El servicio le envía a la plataforma la información cifrada, el algoritmo utilizado y con que clave asimétrica quiere que la descifre.
Tipo:	Primario.
Referencias cruzadas:	Gestionar claves.
Precondiciones	
- El applet debe estar instalado en la tarjeta SIM. - Debe estar almacenada la clave privada del usuario, en el caso correspondiente.	

Flujo Principal
− El servicio le envía a la plataforma la información cifrada, el nombre del algoritmo y como quiere que la descifre. Subflujos S1ó S2. − La plataforma le retorna al servicio la información descifrada.

Subflujos
S1: Descifrar con la clave privada del usuario - La plataforma le ordena a la tarjeta SIM que descifre una información con la clave privada del usuario. - Luego la SIM le retorna la información descifrada a la plataforma. *S2: Descifrar con la clave pública de una entidad conocida* - La plataforma almacena la clave pública de la entidad conocida en la tarjeta SIM. - La plataforma le ordena a la tarjeta SIM que descifre una información con la clave pública de la entidad. - Luego la SIM le retorna la información descifrada a la plataforma.

Flujos de Excepción
E1: No se puede descifrar la información. - La plataforma lanza una excepción debido a tres posibilidades: la información ha sido modificada, la clave no es válida, el algoritmo no es soportado

Información General	
Caso de uso:	**Usar cifrado asimétrico**
Actores:	Servicio
Propósito:	Le permite al servicio cifrar una información con la clave pública o privada del usuario, o cifrar con la clave pública de una entidad.
Resumen:	El servicio le envía a la plataforma una información para que la cifre con alguna de las claves asimétricas almacenadas en la SIM.
Tipo:	Primario.
Referencias cruzadas:	Gestionar clave.
Precondiciones	
- El applet debe estar instalado en la tarjeta SIM. - Debe estar almacenada la clave asimétrica correspondiente.	

Flujo Principal
- El servicio le envía a la plataforma la información a cifrar, el nombre del algoritmo y con que clave quiere que la cifre. - La tarjeta SIM cifra la información con el algoritmo y claves especificadas. La SIM le retorna a la plataforma la información cifrada. - La plataforma le retorna al servicio la información cifrada.

Flujos de Excepción
E1: No se soporta el algoritmo. - La plataforma lanza una excepción debido a que no puede cifrar con el algoritmo especificado.

Información General	
Caso de uso:	**Usar cifrado simétrico**
Actores:	Servicio
Propósito:	Permitirle al servicio cifrar una información con una clave simétrica. Así se logra garantizar la integridad y confidencialidad de la información.

Resumen:	El servicio le envía a la plataforma la información a cifrar, el algoritmo utilizado y con que clave simétrica quiere que la cifre.
Tipo:	Primario.
Referencias cruzadas:	Gestionar claves.

Precondiciones

- El applet debe estar instalado en la tarjeta SIM.
- Debe estar almacenada la clave simétrica correspondiente.

Flujo Principal

- El servicio le envía a la plataforma la información, el nombre del algoritmo y con que clave quiere que la cifre.
- La plataforma obtiene de la tarjeta SIM la respectiva clave. Subflujos S1ó S2.
- La plataforma cifra la información con el respectivo algoritmo.
- La plataforma le envía al servicio la información cifrada.

Subflujos

S1: Obtener la clave simétrica del usuario

- La plataforma le pide a la tarjeta SIM la clave simétrica del usuario.
- La SIM le envía la clave a la plataforma.

S2: Obtener la otra clave simétrica

- La plataforma le pide a la tarjeta SIM la otra clave simétrica.
- La SIM le envía la clave a la plataforma.

Flujos de Excepción

E1: No se puede cifrar la información.

- La plataforma lanza una excepción debido a que el algoritmo no es soportado

Información General

Caso de uso:	**Usar descifrado simétrico**
Actores:	Servicio
Propósito:	Permitirle conocer al servicio si la información que le llegó no ha sido modificada, así se garantiza la integridad y confidencialidad de la información.
Resumen:	El servicio le envía a la plataforma la información cifrada, el algoritmo utilizado y con que clave simétrica quiere que la descifre.
Tipo:	Primario.
Referencias cruzadas:	Gestionar claves.

Precondiciones

- El applet debe estar instalado en la tarjeta SIM.
- Debe estar almacenada la clave simétrica correspondiente.

Flujo Principal

- El servicio le envía a la plataforma la información cifrada, el nombre del algoritmo y con que clave quiere que la descifre.
- La plataforma obtiene de la tarjeta SIM la respectiva clave. Subflujos S1ó S2.
- La plataforma descifra la información cifrada con el respectivo algoritmo.
- La plataforma le envía al servicio la información descifrada.

Subflujos
S1: Obtener la clave simétrica del usuario - La plataforma le pide a la tarjeta SIM la clave simétrica del usuario. - La SIM le envía la clave a la plataforma. *S2: Obtener la otra clave simétrica* - La plataforma le pide a la tarjeta SIM la otra clave simétrica. - La SIM le envía la clave a la plataforma.

Flujos de Excepción
E1: No se puede descifrar la información. - La plataforma lanza una excepción debido a que el algoritmo no es soportado

1.3. Diagramas de secuencia de análisis

Como características adicionales del análisis de la plataforma se tienen:

- Manejar un Applet en la tarjeta SIM encargado de la seguridad y otro Applet encargado de acceder a los parámetros SIM. Esto debido a que el soporte de las características criptográficas del Applet de seguridad pueden no ser cumplidas por todas las tarjetas SIM reales, con lo que en el peor de los casos no se tendrían las características criptográficas de la SIM, pero si se podría acceder a sus parámetros.

- Gestionar dos claves simétricas DES: myDESKey y la clave DES de otra entidad.

- Gestionar tres claves asimétricas RSA: myRSAPublicKey, myRSAPrivateKey y la clave pública de otra entidad.

Caso de uso: Cargar Applet

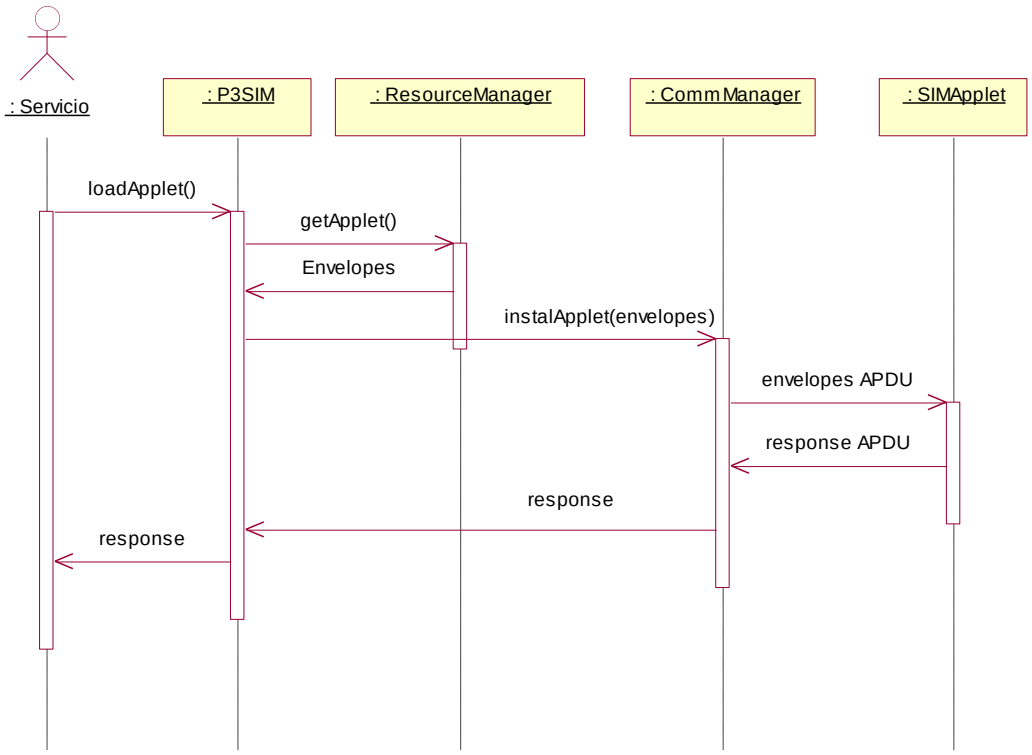

Figura 1-2. Diagrama de secuencia de análisis para Cargar Applet

Caso de uso: Generar firma

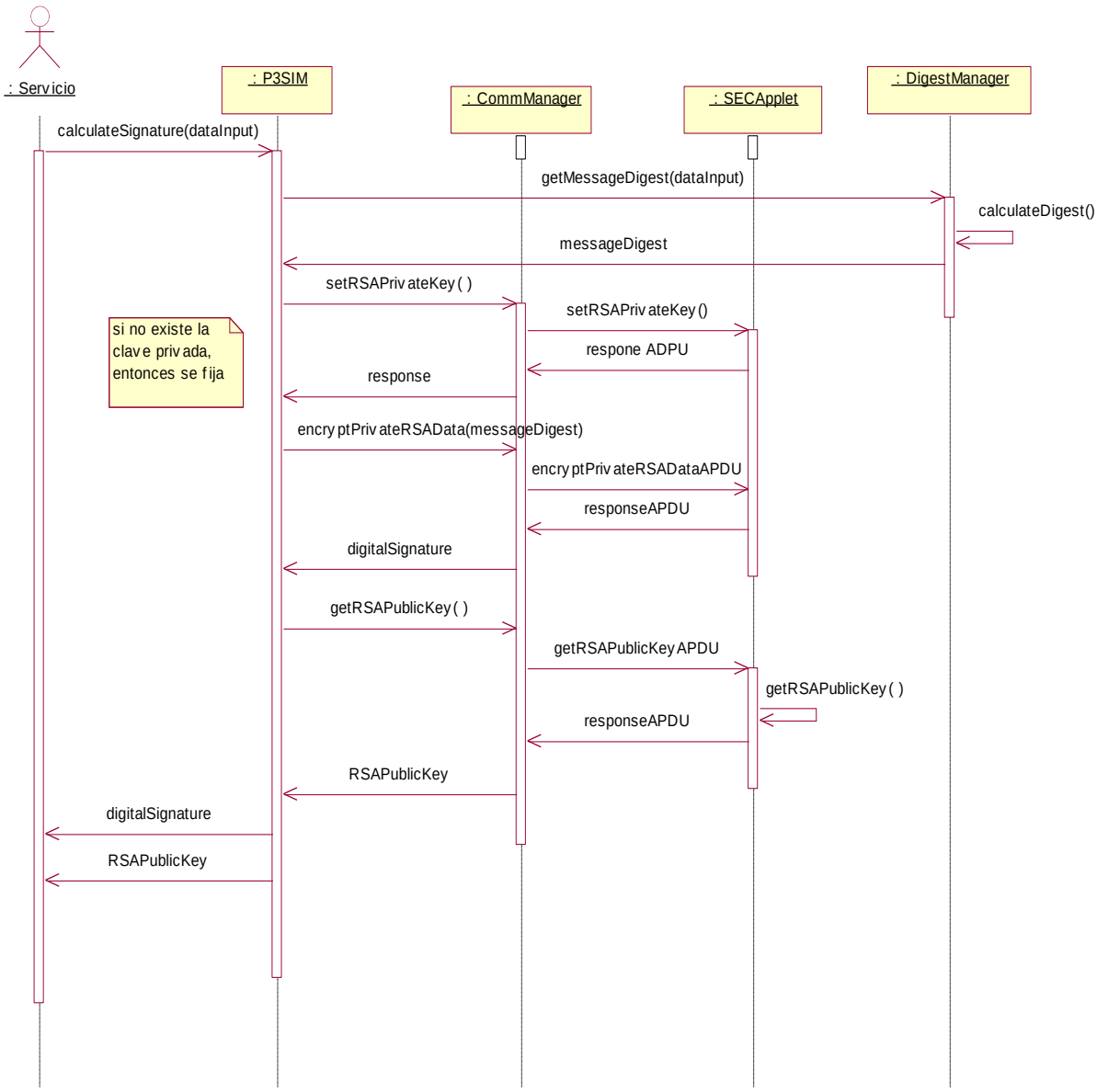

Figura 1-3. Diagrama de secuencia de análisis para Generar firma

Caso de uso: Gestionar clave

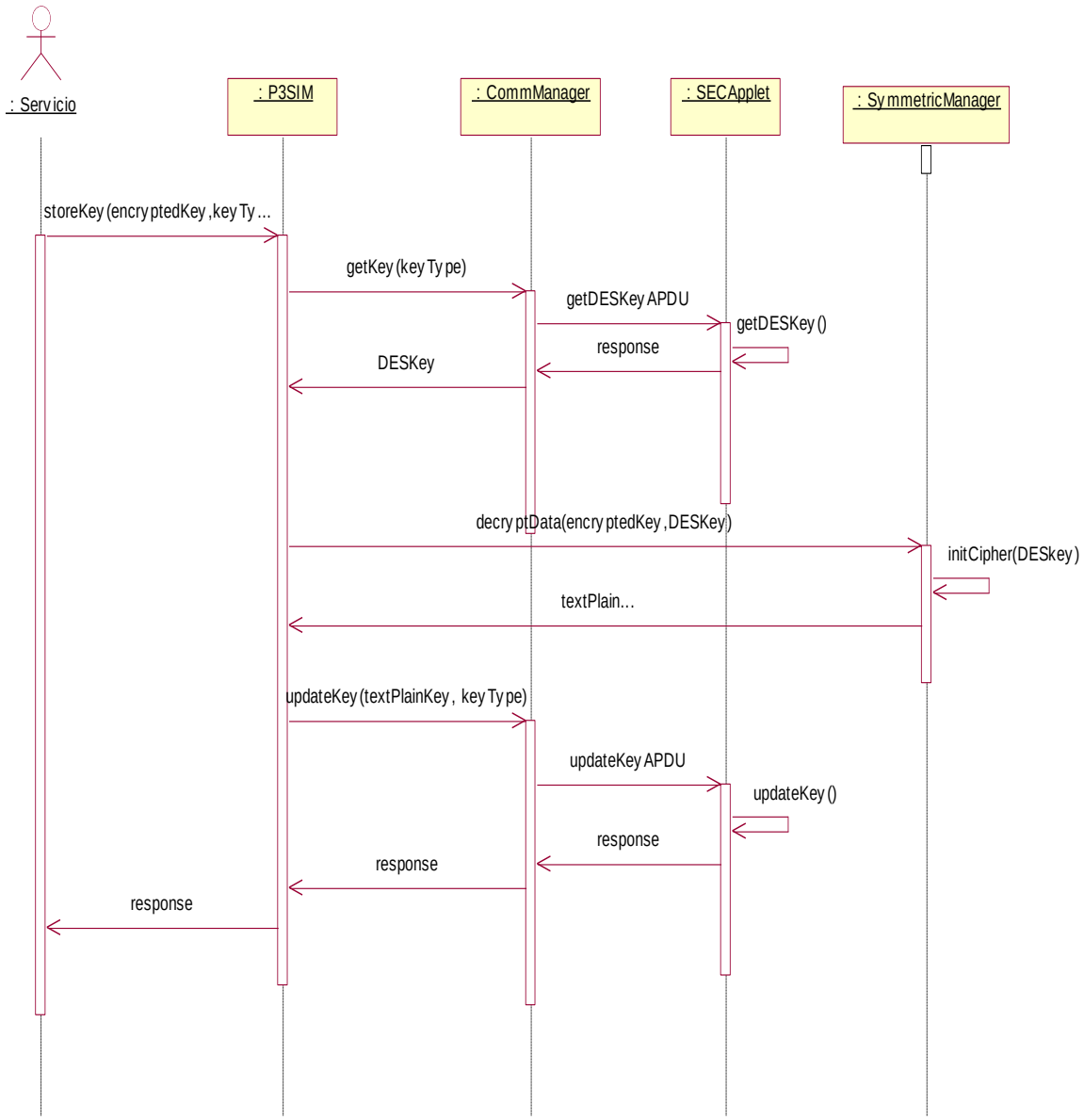

Figura 1-4. Diagrama de secuencia de análisis para Gestionar clave

Caso de uso: Obtener parámetro SIM

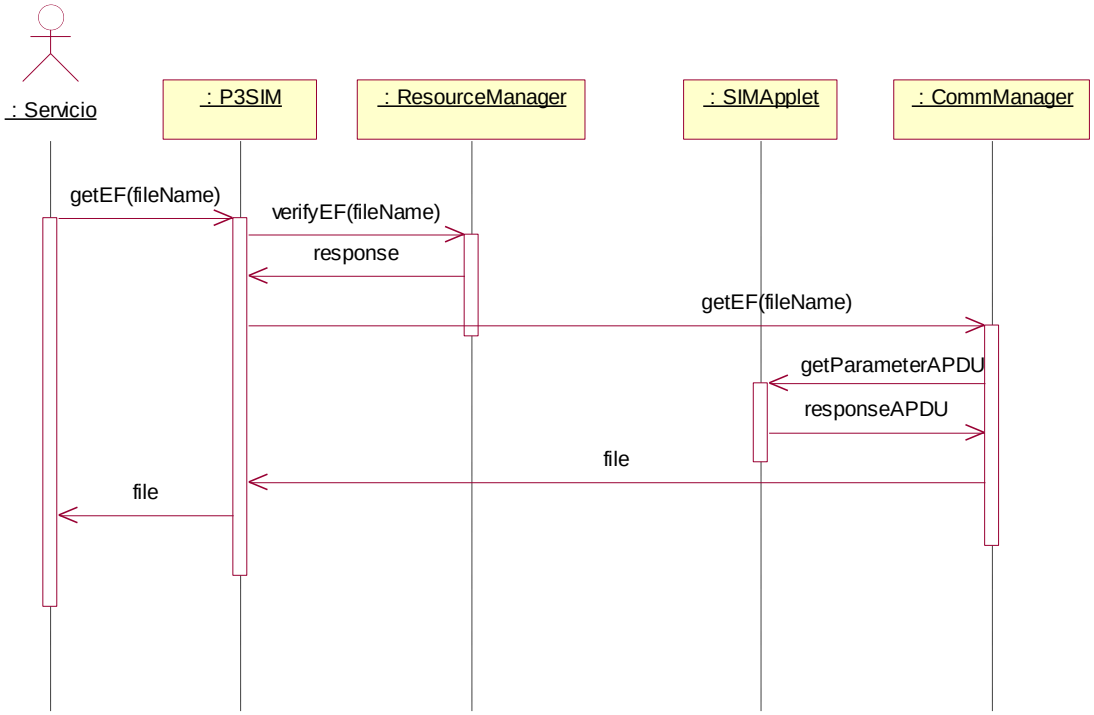

Figura 1-5. Diagrama de secuencia de análisis para Obtener un parámetro SIM

Caso de uso: Usar cifrado asimétrico

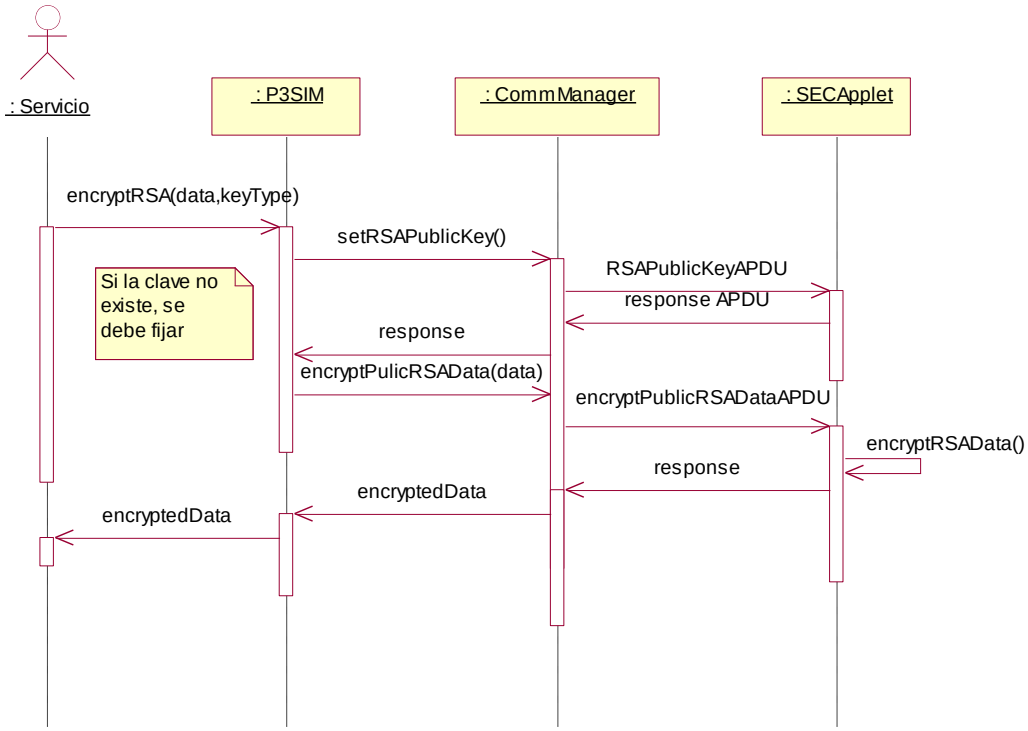

Figura 1-6. Diagrama de secuencia de análisis para Usar cifrado asimétrico

Caso de uso: Usar cifrado simétrico

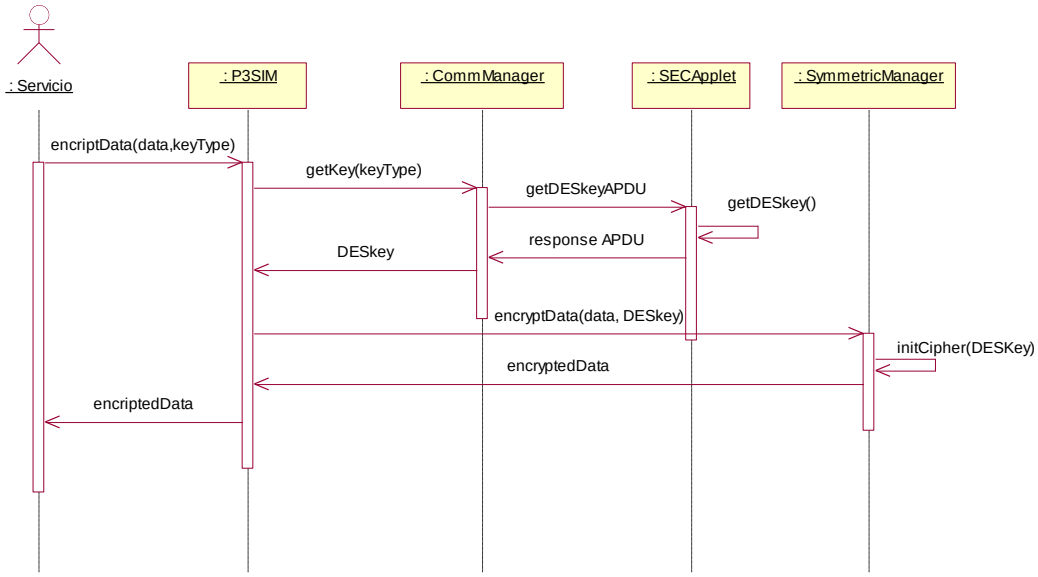

Figura 1-7. Diagrama de secuencia de análisis para Usar cifrado simétrico

Caso de uso: Usar descifrado Asimétrico

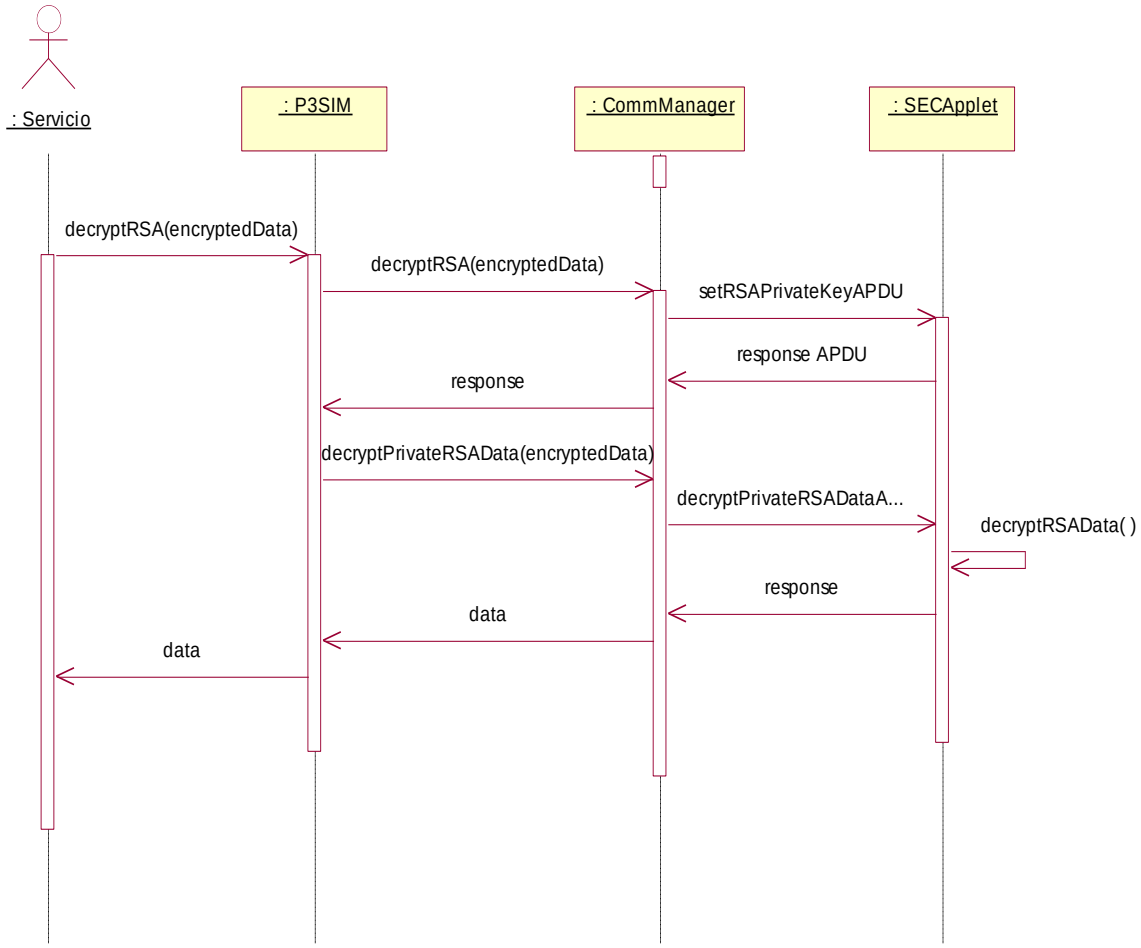

Figura 1-8. Diagrama de secuencia de análisis para Usar descifrado Asimétrico

Caso de uso: Usar descifrado simétrico

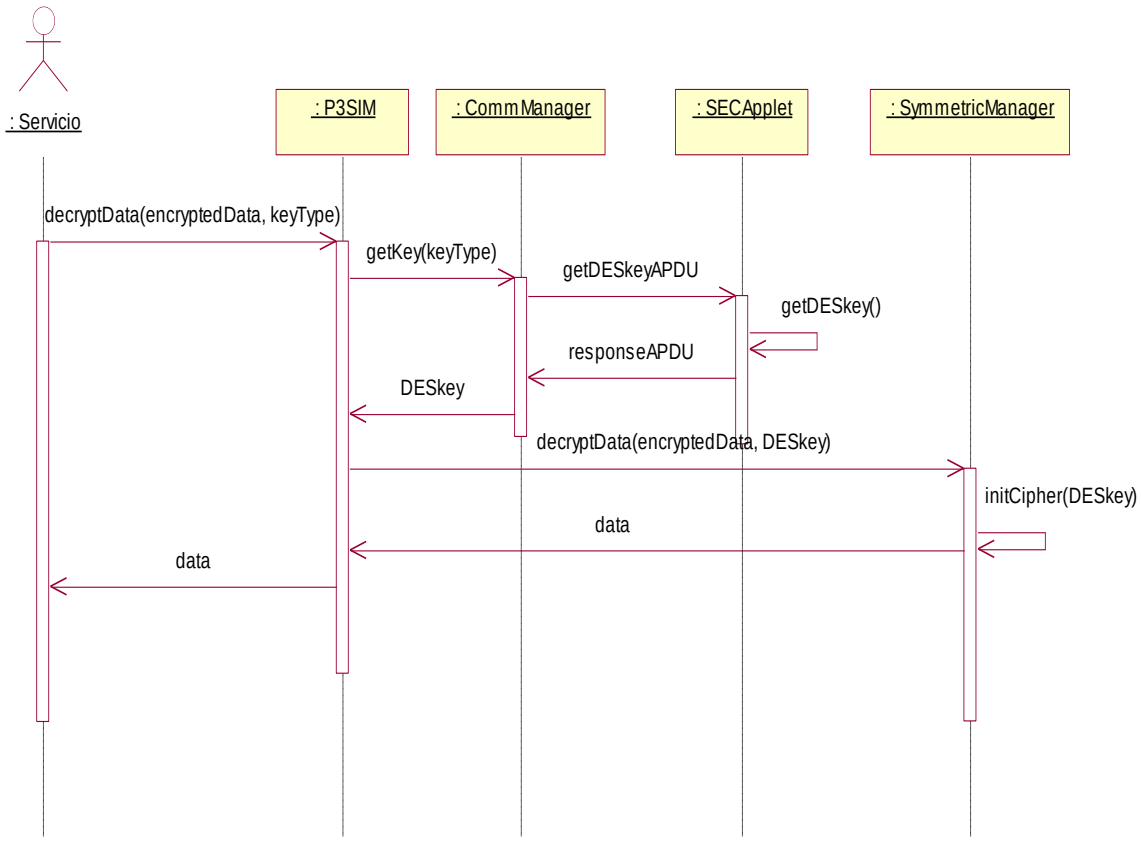

Figura 1-9. Diagrama de secuencia de análisis para Usar descifrado simétrico

Caso de uso: Verificar firma

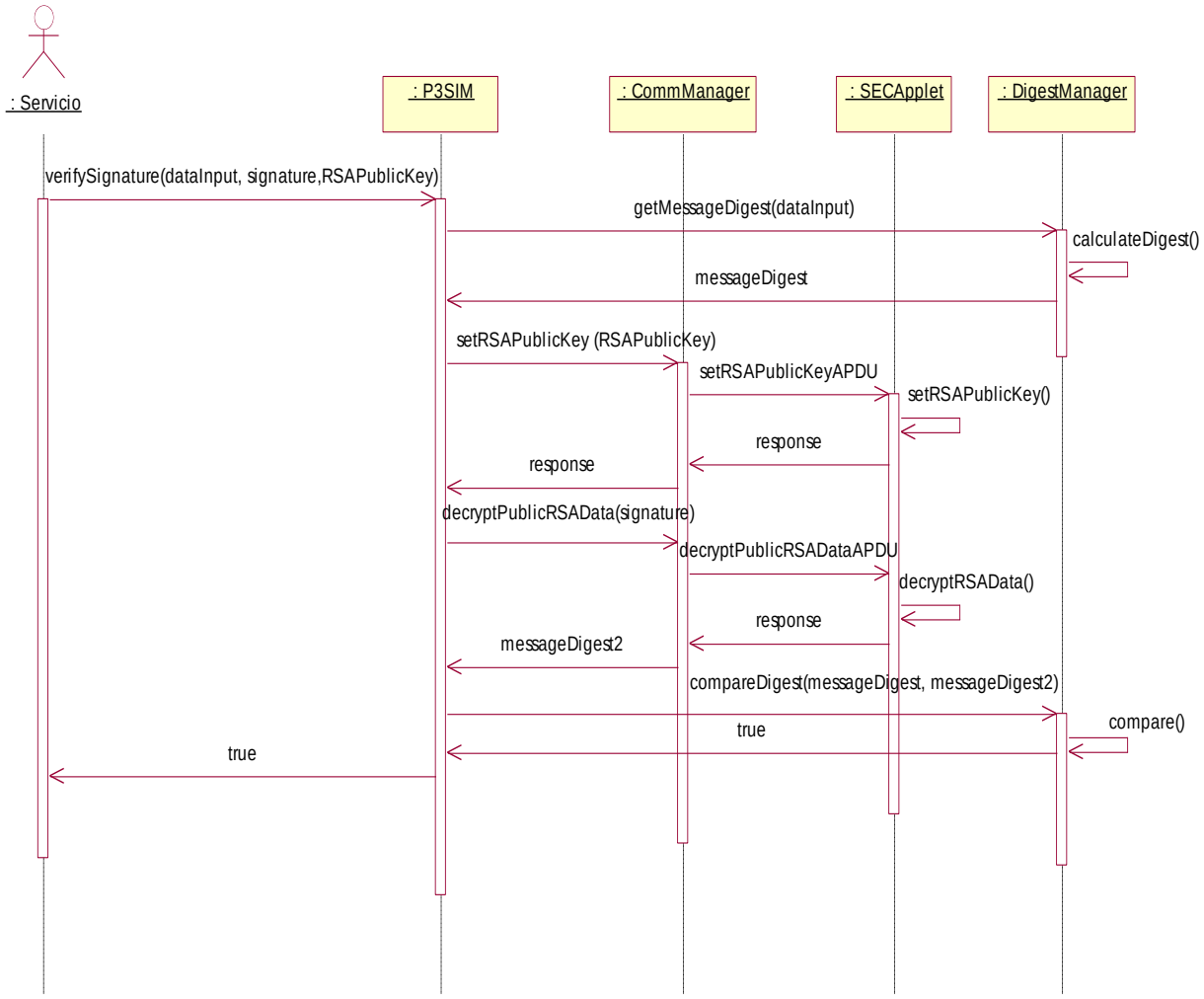

Figura 1-10. Diagrama de secuencia de análisis para Verificar firma

1.4. Diagrama de clases de análisis

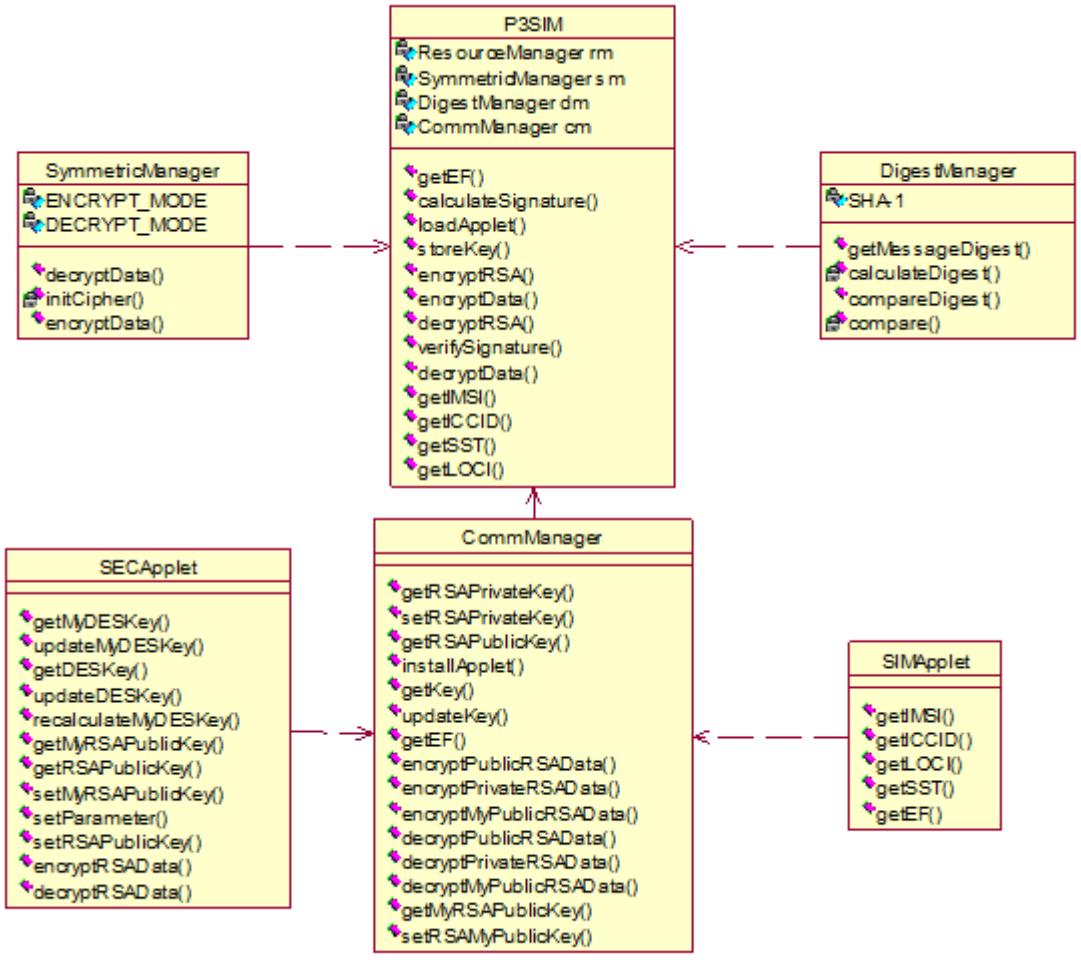

Figura 1-11. Diagrama de clases de análisis

2. DISEÑO

Cuando se paso de la etapa de análisis a la de diseño, se detectaron varios inconvenientes:

- Las claves asimétricas, no se manejan en texto plano, lo que si se puede manejar en texto plano son los parámetros que las generan. Dichos parámetros son: el modulo, el exponente privado y el exponente público. Esos parámetros se deben poder fijar y obtener.

- Por seguridad el exponente privado sólo se debe poder fijar, nunca se debe poder obtener.

- Al trabajar con dos Applets (uno para criptografía y el otro para acceder a los parámetros SIM) se tiene un problema de sincronización, debido a que constantemente se debe cerrar la conexión con uno y abrirla con otro. Por eso se decidió trabajar con un solo applet.

2.1. Diagramas de secuencia

Debido a los argumentos planteados anteriormente, se tienen dos cambios importantes. El primero es que se trabajo con un solo applet, llamado SECApplet. El segundo es que al fijar y obtener una clave asimétrica, lo que se hace es fijar u obtener los parámetros que la generan (el modulo, el exponente público o el exponente privado).

Caso de uso: Cargar Applet

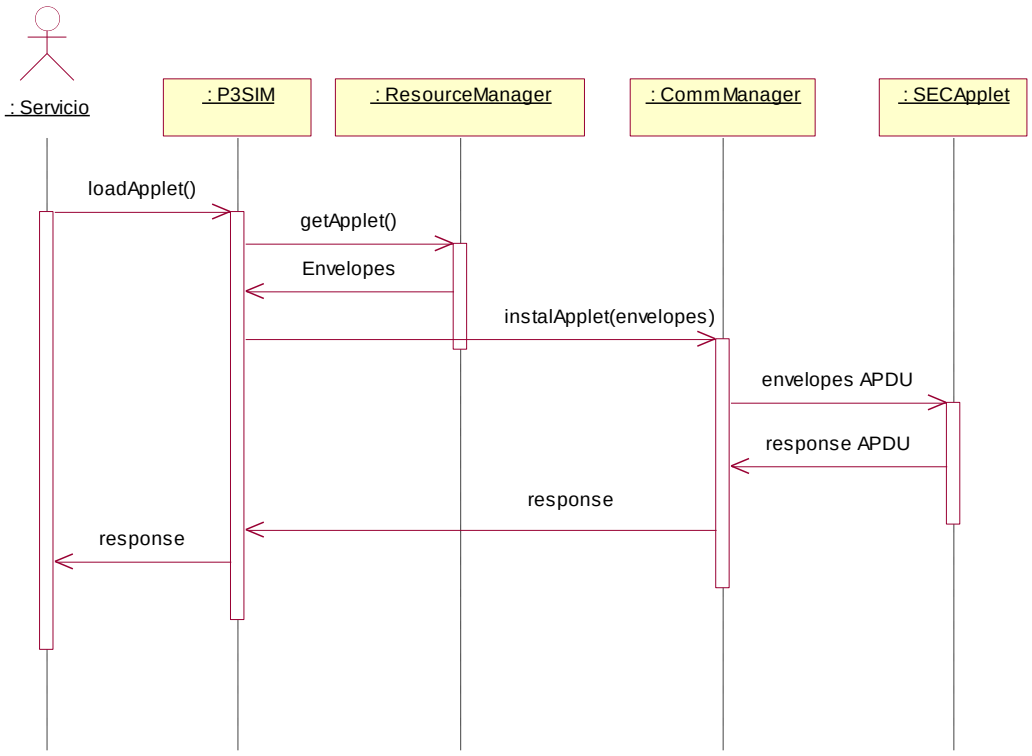

Figura 2-1. Diagrama de secuencia para Cargar Applet

Caso de uso: Generar firma

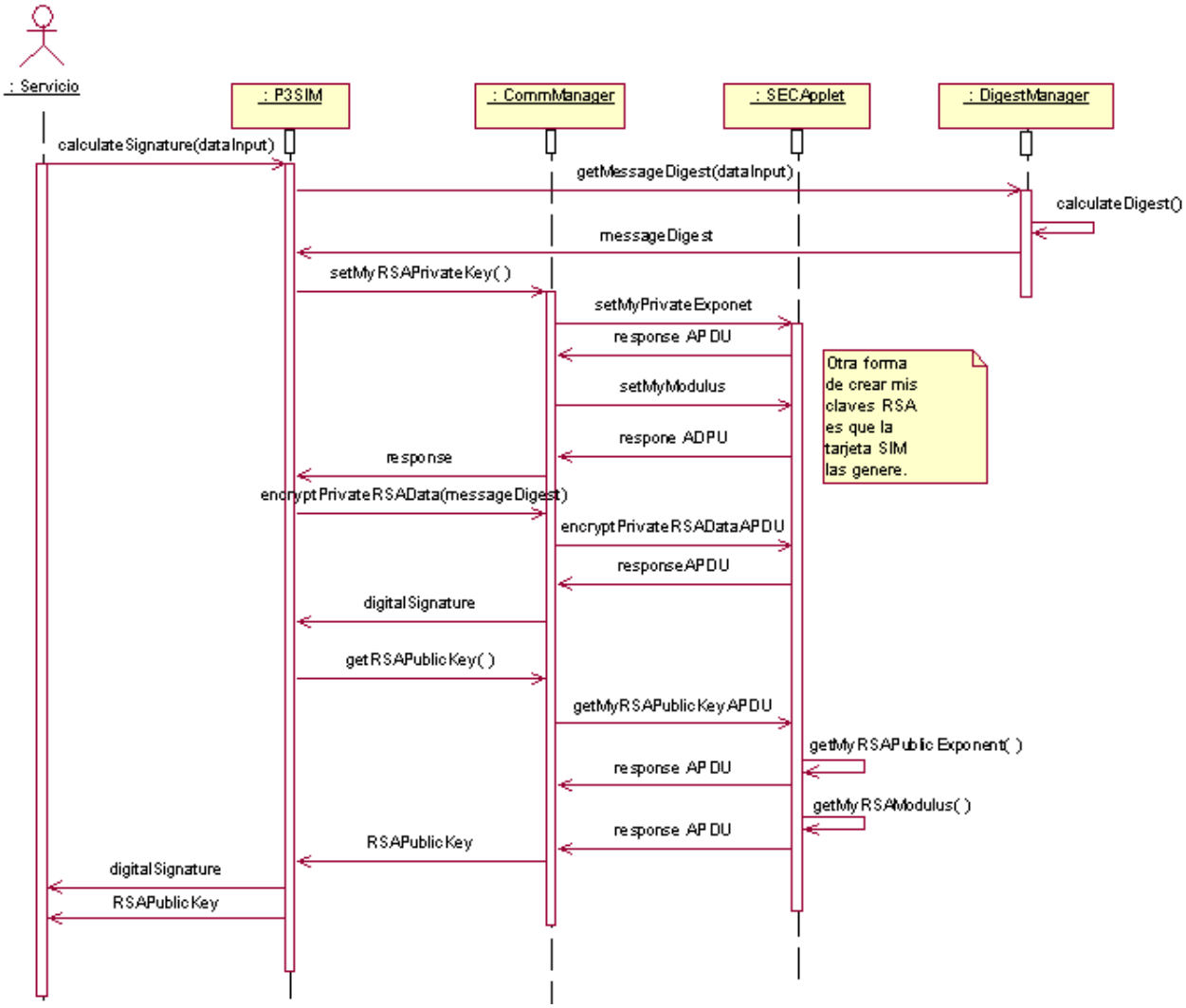

Figura 2-2. Diagrama de secuencia para Generar firma

Caso de uso: Gestionar clave

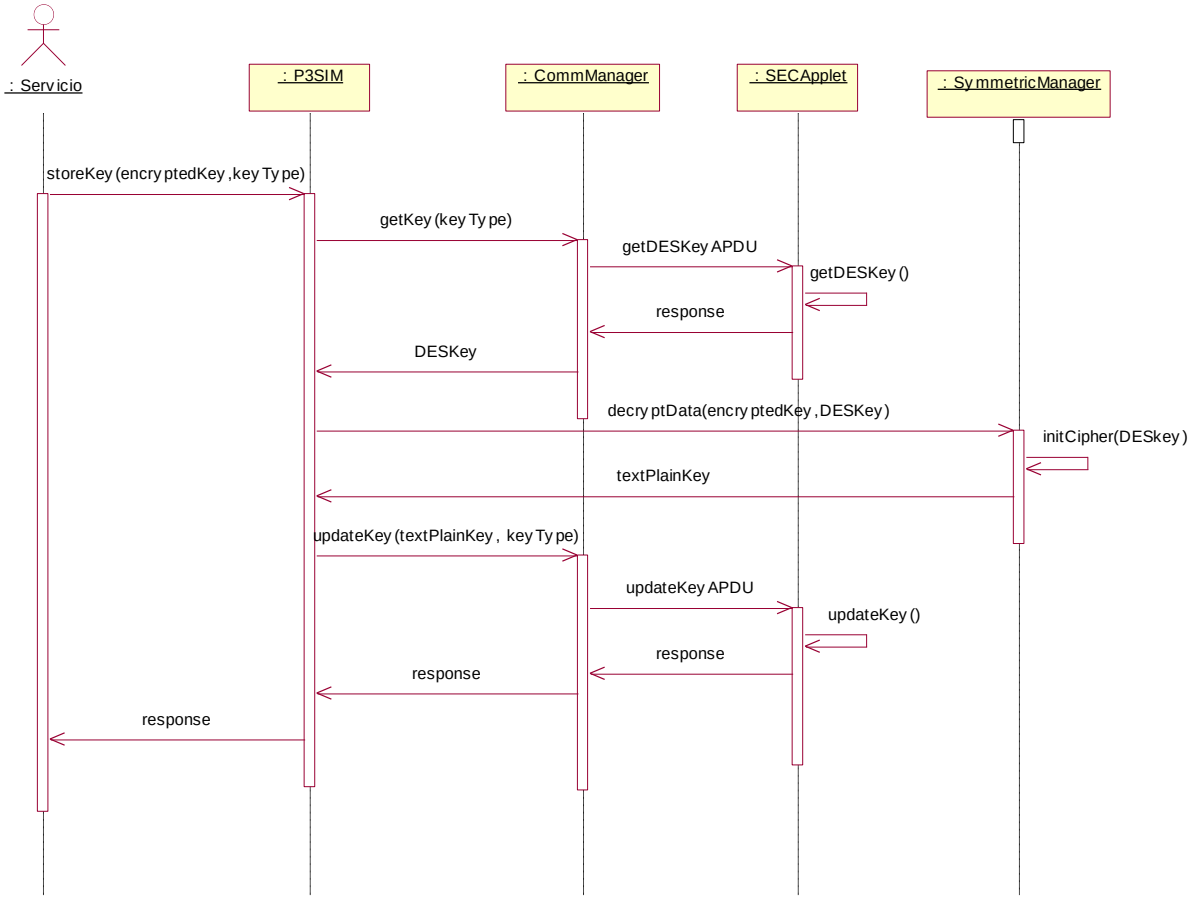

Figura 2-3. Diagrama de secuencia para Gestionar clave

Caso de uso: Obtener parámetro SIM

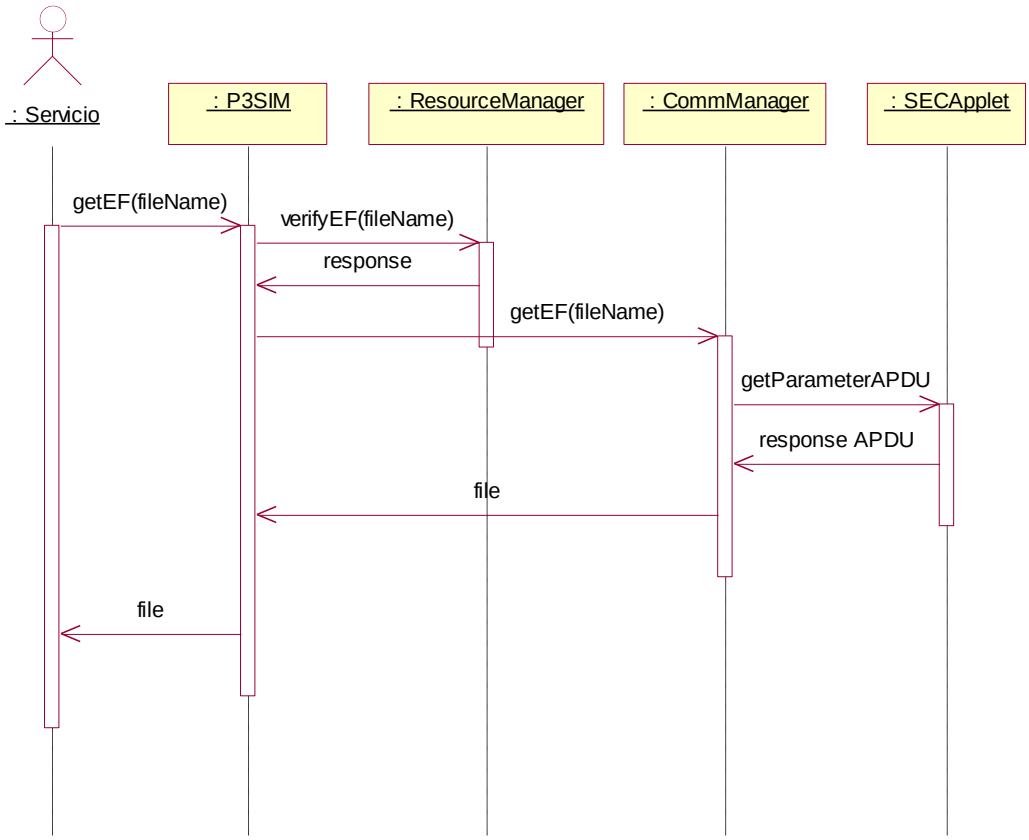

Figura 2-4. Diagrama de secuencia para Obtener parámetro SIM

Caso de uso: Usar cifrado asimétrico

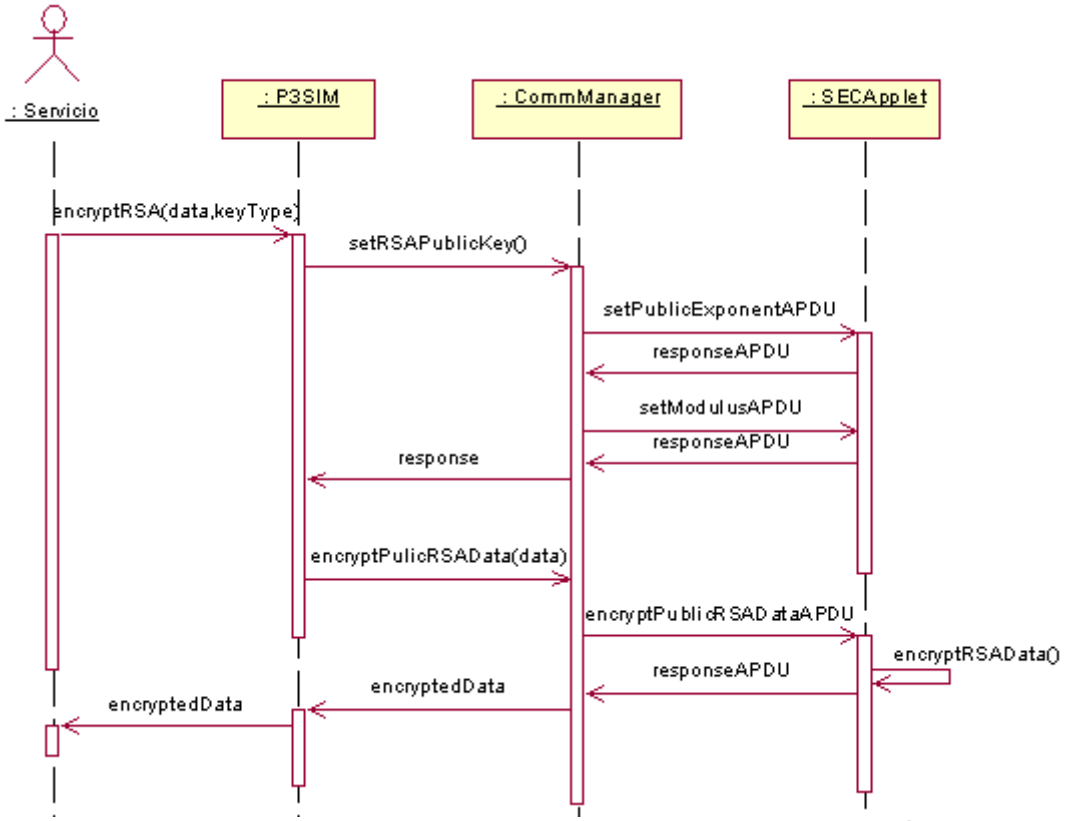

Figura 2-5. Diagrama de secuencia para Usar cifrado asimétrico

Caso de uso: Usar cifrado simétrico

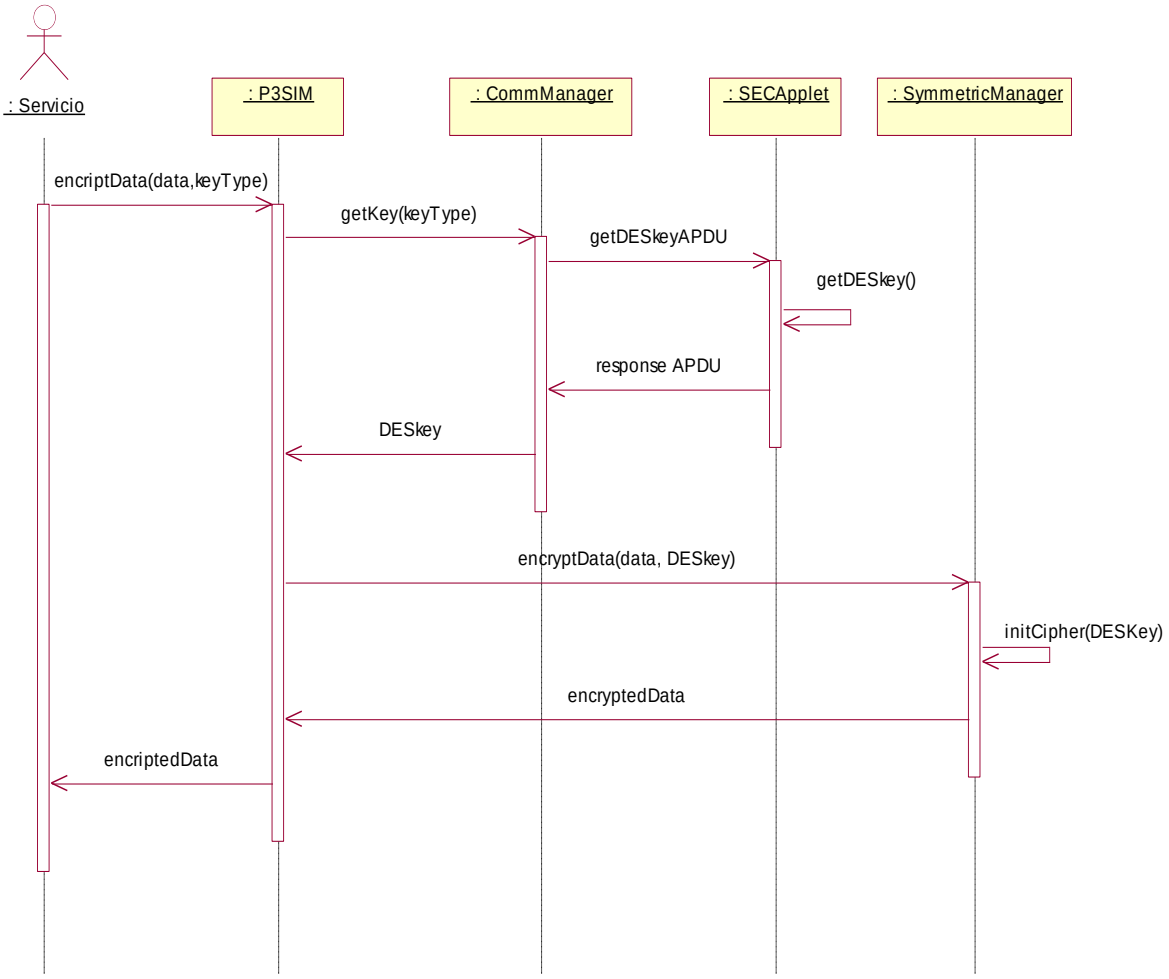

Figura 2-6. Diagrama de secuencia para Usar cifrado simétrico

Caso de uso: Usar descifrado asimétrico

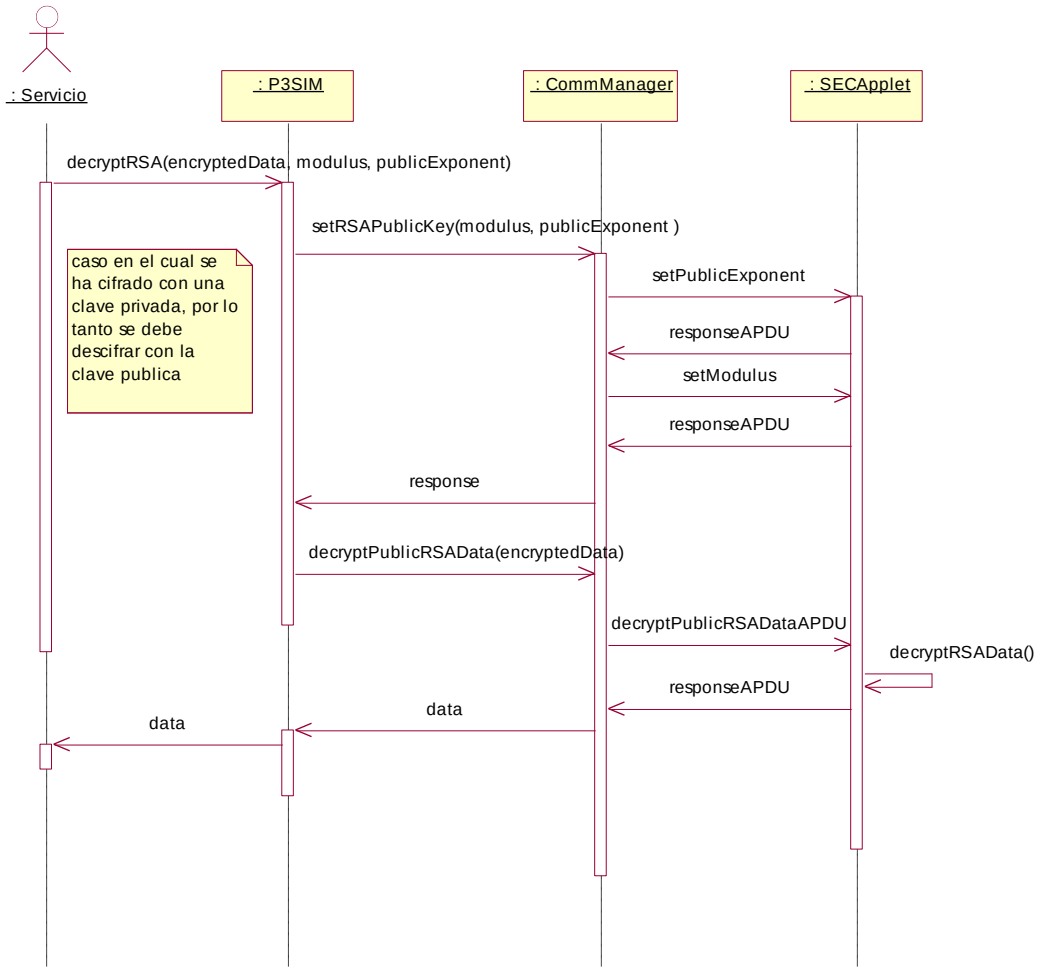

Figura 2-7. Diagrama de secuencia para Usar descifrado asimétrico

Caso de uso: Usar descifrado simétrico

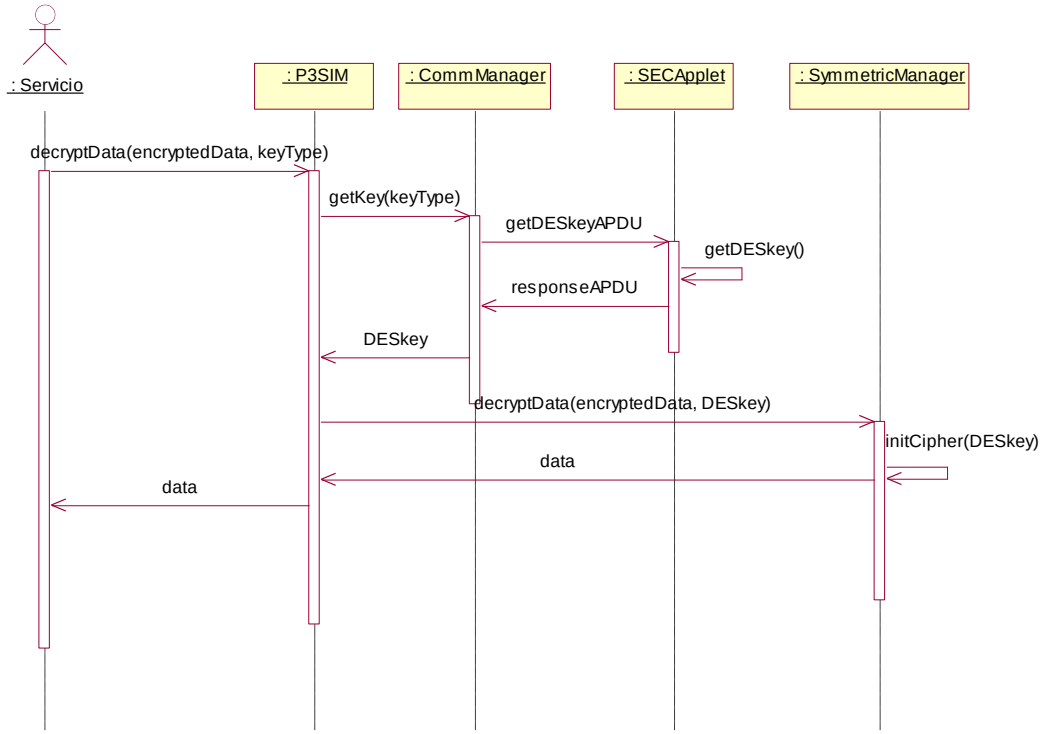

Figura 2-8. Diagrama de secuencia para Usar descifrado simétrico

Caso de uso: Verificar firma

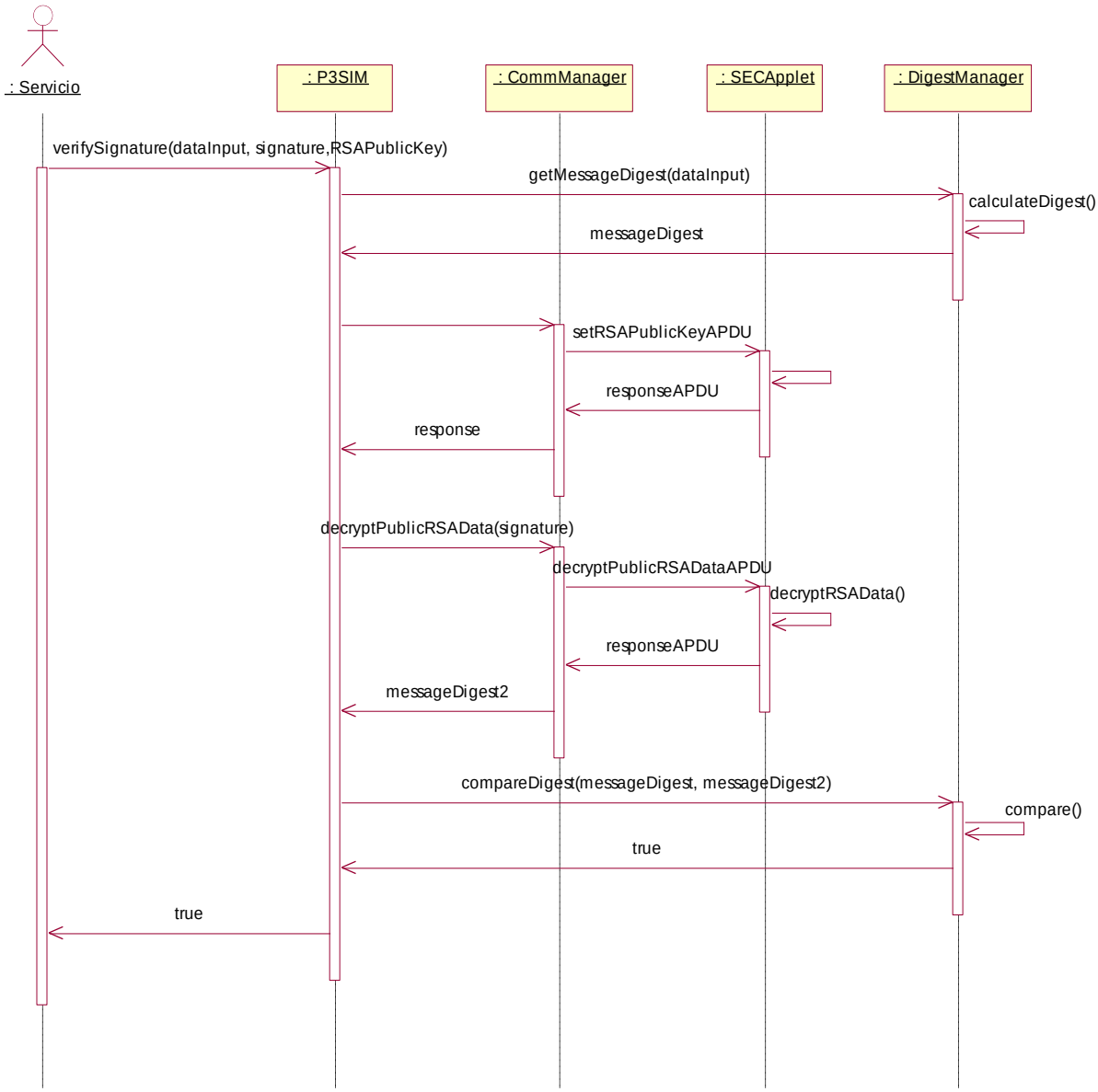

Figura 2-9. Diagrama de secuencia para verificar firma

2.2. Diagramas de clases de la plataforma

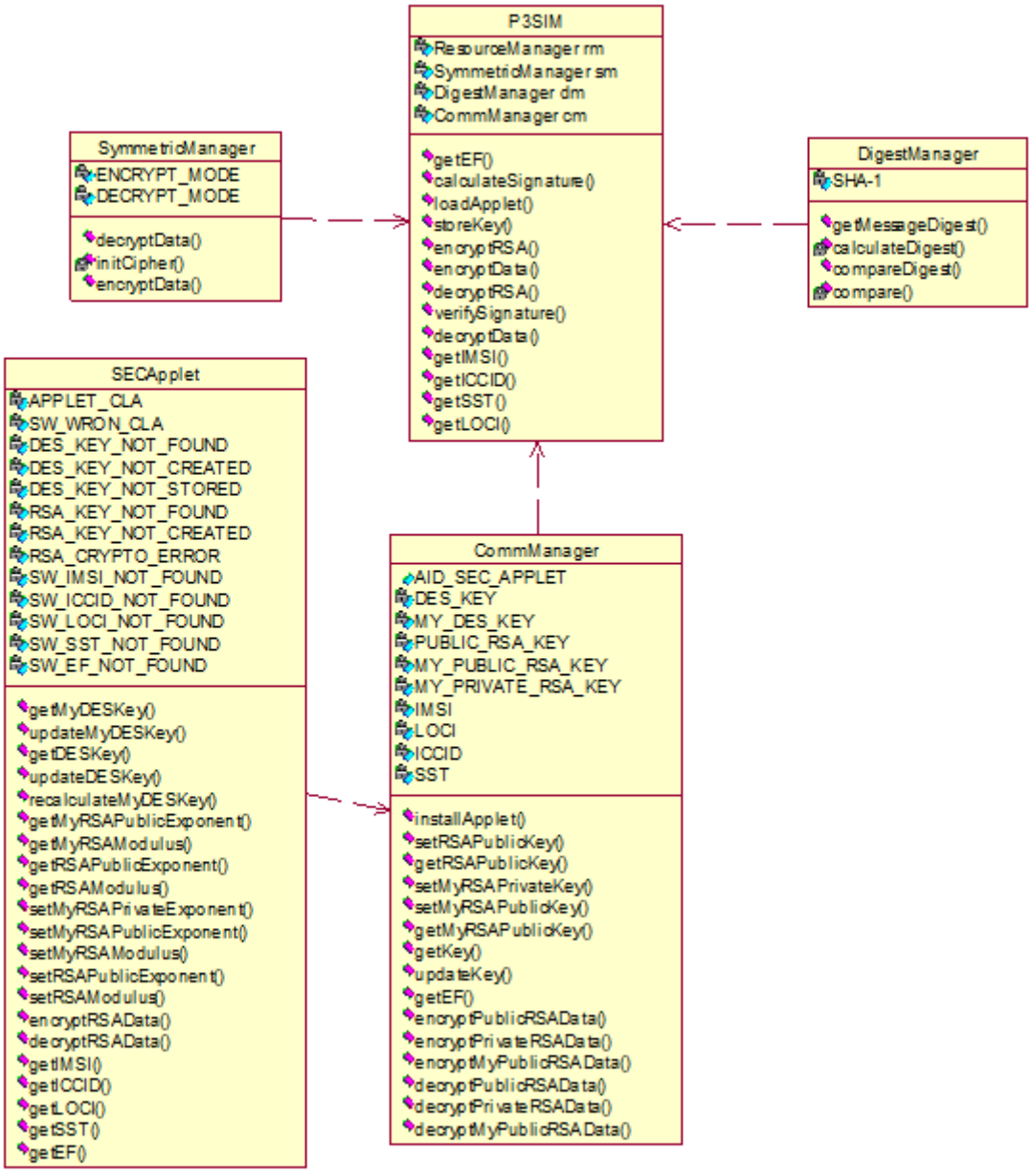

Figura 2-10. Diagrama de clases de la plataforma

2.3. Diagramas de paquetes de la plataforma

La plataforma consta de 2 paquetes y una carpeta de recursos. En el paquete control se encuentra la clase P3SIM. En el paquete beans se encuentran las clases DigestManager, SymmetricManager y CommManager. La carpeta resource contiene un archivo de texto que tiene las APDUs que permitirán instalar el SECApplet en la tarjeta SIM. La figura 2-11 muestra las relaciones entre los paquetes.

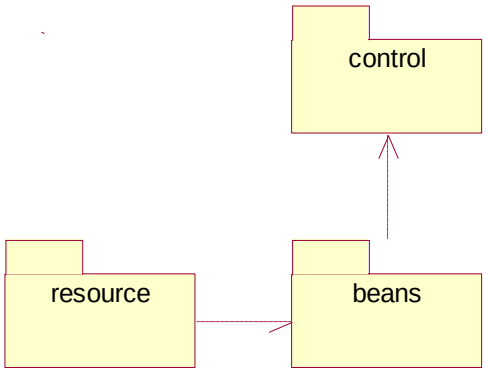

Figura 2-11. Diagrama de paquetes de la plataforma