UNIVERSIDAD NACIONAL DE INGENIERÍA

FACULTAD DE INGENIERÍA ELÉCTRICA Y ELECTRÓNICA

ESTUDIO DEL ALGORITMO DE ENCRIPTAMIENTO RSA Y TRIPLE DES PARA MENSAJES FINANCIEROS BASADO EN UN MÓDULO DE SEGURIDAD DE HARDWARE UTILIZADO EN LAS TRANSFERENCIAS INTERBANCARIAS

INFORME DE SUFICIENCIA

PARA OPTAR EL TÍTULO PROFESIONAL DE:

INGENIERO ELECTRÓNICO

PRESENTADO POR:

PERCY FÉLIX MARTÍNEZ GARCÍA

PROMOCIÓN
1996 - I

LIMA – PERÚ
2011

ESTUDIO DEL ALGORITMO DE ENCRIPTAMIENTO RSA Y TRIPLE DES PARA MENSAJES FINANCIEROS BASADO EN UN MÓDULO DE SEGURIDAD DE HARDWARE UTILIZADO EN LAS TRANSFERENCIAS INTERBANCARIAS

Dedicado a mi padres
Donato y Segundina

Y a mis hermanos
Benito y Henry

SUMARIO

El presente trabajo estudia los algoritmos de encriptamiento aplicados a los mensajes financieros que son intercambiados entre las instituciones financieras, con la finalidad de garantizar la seguridad de su información. En este caso, el presente trabajo comprende a las instituciones financieras que pertenecen a una red de comunicaciones financieras a nivel mundial llamado SWIFT (Society for Worldwide Interbank Financial Telecommunication).

En el desarrollo del presente trabajo se describe a los algoritmos de encriptamiento empleados para dar protección a la información de los mensajes financieros, los cuales son el algoritmo asimétrico RSA (el nombre se debe a sus tres inventores: Rivest, Shamir y Adleman) y el algoritmo simétrico triple DES (Data Encryption Standard).

También se describe un módulo de seguridad de hardware (HSM, Hardware Security Module), que es el dispositivo encargado de realizar todas las operaciones criptográficas sobre los mensajes financieros, aplicando los respectivos algoritmos de encriptamiento. Además, este dispositivo crea, almacena y protege las claves criptográficas que son necesarias para todas estas operaciones criptográficas.

ÍNDICE

INTRODUCCIÓN

Hoy en día a nivel mundial se realizan a diario millones de intercambios de mensajes financieros entre las instituciones financieras, donde cada mensaje contiene información confidencial o privilegiada sobre la situación financiera del sector, y puede representar el movimiento de grandes cantidades de dinero. Por lo tanto, es de gran importancia de que esa información se encuentre totalmente protegida y asegurada.

Estas instituciones financieras se interconectan a través de una red de comunicaciones financieras a nivel mundial llamado SWIFT (Society for Worldwide Interbank Financial Telecommunication), el cual se encarga de suministrar la plataforma de comunicación privada, que permite que sus clientes puedan conectarse e intercambiar información financiera con seguridad y de forma fiable. SWIFT es únicamente un transmisor de mensajes y no almacena información financiera de forma permanente. Al actuar como transmisor, sirve de vehículo para los mensajes transmitidos entre dos instituciones financieras. Esta actividad implica el intercambio seguro de datos privados, al tiempo que se garantiza su confidencialidad e integridad [14].

Para dar protección y seguridad a la información del mensaje se procede a encriptarlo, el cual es un proceso de convertir el texto original del mensaje en un texto ilegible, de tal forma que si este mensaje es interceptado por terceros, éste no pueda ser entendido (es decir, nadie salvo el destinatario puede descifrarlo). En este contexto, existen tres grandes grupos de criptografía [9][11]:

- Criptografía simétrica: es un método criptográfico que usa una misma clave para cifrar y descifrar los mensajes. Las dos partes que se comunican han de ponerse de acuerdo sobre la clave común a usar. Una vez que ambas partes tienen acceso a la misma clave, el remitente cifra un mensaje usando la clave, lo envía al destinatario, y éste lo descifra con la misma clave.
- Criptografía asimétrica: es un método criptográfico que usa un par de claves (pública y privada) para el envío de mensajes. Las dos claves están relacionadas y pertenecen a la misma institución. Una clave es pública y se publica para que las demás instituciones financieras tengan conocimiento de ella, la otra clave es privada y la institución financiera propietaria debe guardarla de tal forma que nadie tenga acceso a ella. Las dos principales aplicaciones de la criptografía asimétrica son:

Si el remitente usa la clave pública del destinatario para cifrar el mensaje, y una vez cifrado el mensaje, sólo el destinatario podrá descifrar este mensaje, ya que es el único que conoce la clave privada. Por tanto se logra la confidencialidad del mensaje.

Si el remitente usa su clave privada para cifrar el mensaje, cualquiera puede descifrarlo usando la clave pública del remitente. En este caso se consigue la identificación y autentificación del remitente, debido a que sólo pudo haber sido él quien usó su clave privada. Esta es la base del fundamento de la firma digital.

- Criptografía híbrida: es un método criptográfico que usa tanto el cifrado simétrico como el cifrado asimétrico. El cifrado asimétrico se usa para compartir una misma clave simétrica entre dos instituciones. Y el mensaje que se envía se cifra y descifra con esta clave simétrica.

Cada institución financiera emplea la criptografía con la finalidad de garantizar la seguridad de la información de todos sus mensajes financieros. Para ello, estas instituciones financieras utilizan unos dispositivos de hardware dedicados a realizar todas estas operaciones criptográficas, siendo estos dispositivos los módulos de seguridad de hardware (HSM, Hardware Security Module).

El HSM es un dispositivo basado en hardware que genera, almacena y protege las claves criptográficas; y suele aportar una aceleración hardware para las operaciones criptográficas de alto rendimiento que se efectúan dentro del mismo dispositivo. También proporciona una protección lógica y física contra el acceso no autorizado, por ello aumenta significativamente la seguridad en comparación con otros dispositivos que almacenan información. El HSM almacena y protege las claves privadas y las claves simétricas [2][12].

Las claves públicas de todas las instituciones financieras son almacenadas en el directorio de la red SWIFT, el cual es un componente administrado por SWIFTNet PKI (SWIFTNet Public Key Infrastructure), que es una infraestructura de clave pública de la red SWIFT. Por tanto SWIFTNet PKI garantiza que una clave pública es correcta, que pertenece a la institución y que no ha sido manipulado o reemplazado por un tercero [1].

El presente trabajo está constituido de 4 capítulos, los cuales serán resumidos a continuación:

- El capítulo I "Definición del problema", se refiere a la importancia de mantener segura la información del mensaje financiero que se intercambia entre las instituciones financieras. Por ello, se tiene que garantizar la seguridad de su información, manteniendo su confidencialidad, autenticidad, integridad y no repudio en el intercambio [11].
- El capítulo II "Marco teórico", como el presente trabajo comprende solo a las instituciones financieras que pertenecen a la red de comunicaciones financieras SWIFT,

se explica lo referente a ese marco, como: la conectividad a la red SWIFT, la identificación de una institución financiera por medio de su código BIC, la elaboración de un mensaje financiero y la infraestructura de clave pública de la red SWIFT [14][15].

- El capítulo III “Metodología de solución”, se refiere a los elementos a emplear para dar una mayor protección y seguridad al mensaje financiero, los cuales son [2][9]:

El HSM, tipos de HSM, acceso seguro a las cajas HSM, clúster de las cajas HSM y usuarios de las cajas HSM.

Encriptamiento: algoritmo RSA, algoritmo triple DES

Firma digital: algoritmos RSA, función hash

- El capítulo IV “Estudio de caso”, se refiere a como un mensaje financiero pasa por las diferentes etapas para obtener protección y llegue intacto a su destino.

CAPÍTULO I
DEFINICIÓN DEL PROBLEMA

1.1 Descripción del problema

Las instituciones financieras transmiten mensajes con información confidencial sobre su situación financiera. Por ello, en caso de que los mensajes sean capturados; la institución corre el riesgo de que la información sea utilizada maliciosamente y finalmente sean causas de la pérdida de credibilidad, pérdida de negocios, demandas legales o incluso la quiebra de la misma institución.

En la actualidad existen muchos medios de transmisión de ataques a los sistemas de seguridad que se da al mensaje financiero; esto se debe a la infinidad de formas de tener acceso a los recursos informáticos de forma remota y también al incremento de las conexiones a internet. Por ello, los riesgos informáticos que presentan los mensajes financieros han crecido en tamaño, forma y variedad con el uso de la tecnología.

Para garantizar la seguridad de la información de los mensajes financieros intercambiados entre las instituciones financieras y/o los usuarios, se debe considerar lo siguiente [11]:

a) La confidencialidad
b) La autenticación
c) La integridad
d) La no repudiación

a) La confidencialidad

La confidencialidad se logra cuando el mensaje es cifrado y luego enviado por el emisor hasta que llegue a su destino, donde el receptor es el único que puede descifrarlo. Por ello, el cifrado del mensaje previene de cualquier agente no autorizado de poder leerlo, y así asegura su confidencialidad.

b) La autenticación

La autenticación es la confirmación de la identidad del remitente del mensaje. Es una validación de identificación, es decir, es la técnica mediante la cual un proceso comprueba que el remitente es quien se supone que es y no se trata de un impostor.

c) La integridad

La integridad da la seguridad de que los datos no han sido modificados. La integridad de un mensaje se obtiene adjuntándole otro conjunto de datos de comprobación de la integridad.

d) La no repudiación

La no repudiación se logra cuando el remitente no puede negar haber escrito el mensaje una vez este ha sido enviado. Es decir, el emisor no puede negar que lo envió, porque el destinatario tiene pruebas del envío, el receptor recibe una prueba infalsificable del origen del envío, lo cual evita que el emisor, de negar tal envío, tenga éxito ante el juicio de terceros.

1.2 Objetivo del trabajo

Las operaciones interbancarias requieren altos niveles de seguridad, debido a que usualmente son sensibles a ataques por software o hardware. En este sentido, es de interés establecer sistemas de seguridad basadas en técnicas de encriptamiento que tornen seguros y fiables los sistemas financieros.

Por ello, el objetivo del presente trabajo es garantizar la confidencialidad, la autenticidad, la integridad y el no repudio del mensaje financiero que se intercambia entre instituciones financieras a nivel mundial a través de un sistema de comunicaciones seguro [11]. En el presente trabajo, el sistema de comunicaciones financieras a emplear es SWIFT, el cual es totalmente estable (incluyendo sus sistemas de contingencia), con capacidad para intercambiar información con total seguridad y de forma fiable [14].

1.3 Evaluación del problema

La seguridad de la información de un mensaje financiero que es intercambiado entre instituciones financieras tiene un efecto significativo respecto a su confidencialidad y privacidad, la que puede cobrar una gran dimensión dependiendo del contenido del mismo, es decir un mensaje por ejemplo puede representar una transferencia de pago de una gran cantidad de dinero. Por ello, la seguridad de la información ha crecido y evolucionado considerablemente, convirtiéndose en una carrera importante y acreditada a nivel mundial.

Al incrementarse el alcance de la tecnología, el cuidado de la información se ha vuelto crucial para las instituciones financieras, por ello para garantizar la confidencialidad, la autenticidad, la integridad y el no repudio de un mensaje financiero que es intercambiado se aplica los métodos de encriptamiento y de la firma digital [11]:

- La confidencialidad: método de encriptamiento
- La autenticación: método de la firma digital
- La integridad: método de la firma digital
- La no repudiación: método de la firma digital

1.4 Limitaciones del trabajo

El presente trabajo se limita al estudio de un sistema de encriptamiento del mensaje financiero para otorgarle protección y seguridad a su información cuando se intercambia entre las instituciones financieras. Este sistema de encriptamiento se establece dentro del sistema de comunicaciones financieras SWIFT, utilizando los módulos de seguridad de hardware (HSM) [2].

CAPÍTULO II
MARCO TEÓRICO

Debido a que el presente trabajo solo comprende a las instituciones financieras que pertenecen a una red de comunicaciones financieras a nivel mundial llamado SWIFT, se procede a explicar lo referente a este marco que es SWIFT, donde cada institución financiera es identificada por su código BIC (Business Identifier Code).

2.1 Sociedad de telecomunicaciones financieras interbancarias mundiales (SWIFT)

La sociedad de telecomunicaciones financieras interbancarias mundiales (SWIFT) permite al sector financiero llevar a cabo sus operaciones de negocios de forma rápida, segura y fiable [14].

SWIFT permite a sus clientes automatizar y estandarizar las transacciones financieras y, de este modo, reducir tanto los gastos como el riesgo operativo y eliminar ineficiencias en sus operaciones. El uso de SWIFT les ofrece la posibilidad de generar nuevas oportunidades comerciales y flujos de ingresos.

SWIFT tiene su sede central en Bélgica y cuenta con oficinas en los principales centros financieros y mercados en desarrollo del mundo.

Más de 9000 instituciones financieras de 209 países confían en SWIFT a diario para intercambiar millones de mensajes financieros estandarizados.

Misión

La misión de SWIFT es doble [14]:

- Suministrar la plataforma de comunicación privada, donde sus productos y servicios permiten que sus clientes puedan conectarse e intercambiar información financiera con seguridad y de forma fiable.
- Actúa como catalizador, al reunir a la comunidad financiera para colaborar con vistas (propuestas) a adaptar las prácticas del mercado, definir las normas y estudiar soluciones a problemas de interés común.

Supervisión

SWIFT es una sociedad cooperativa sujeta a la legislación de Bélgica y sus accionistas son los propietarios y quienes la controlan [14].

SWIFT tiene el compromiso de mantener un diálogo abierto y constructivo con las autoridades supervisoras. El Banco Nacional de Bélgica, el banco central del país en el

cual SWIFT posee su sede, actúa como supervisor principal, apoyado por los bancos centrales de los países del G-10. La supervisión se concentra en primer lugar en asegurar que SWIFT cuente con controles y procesos efectivos para evitar poner en riesgo la estabilidad financiera y la solidez de las infraestructuras financieras.

Los aspectos tratados pueden incluir todos los temas relacionados con el riesgo sistemático, confidencialidad, integridad, disponibilidad y estrategia de la empresa. SWIFT se somete a supervisión debido a su importancia de hacer que todo el sistema financiero internacional funcione sin problemas, ya que desempeña la función de proveedor de servicios de mensajería.

Los objetivos de la supervisión de SWIFT se centran en la seguridad, la fiabilidad operacional, la continuidad de la empresa y la redundancia de la infraestructura de SWIFT.

2.2 Sistema de comunicaciones SWIFT

El sistema de comunicaciones SWIFT se encuentra controlado por los siguientes tres componentes [3]:

a) Cliente (instituciones financieras)

b) Network Partner

c) SWIFT

La Figura 2.1 ilustra los tres componentes que controlan el sistema de comunicaciones SWIFT, y en el lado del cliente se observa a los HSM que son los dispositivos que realizan todas las operaciones criptográficas sobre el mensaje financiero.

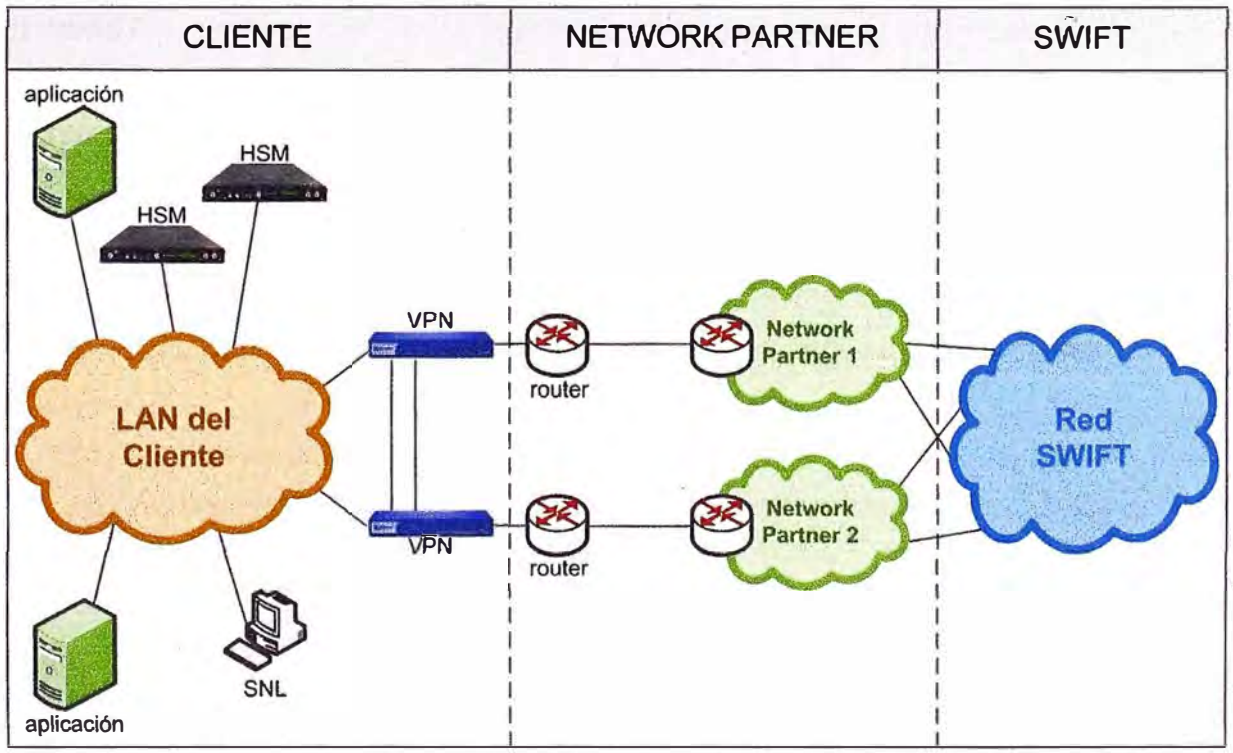

Figura 2.1 - Sistema de comunicaciones SWIFT

a) Cliente (instituciones financieras)

Vienen a ser las instituciones financieras, quienes se encargan de enviar y recibir los mensajes financieros.

Como se observa en la Figura 2.1, en el cliente se encuentran los HSM, por tanto es el lugar donde se realiza el proceso de encriptamiento de los mensajes financieros. También se encuentra el SNL (SWIFTNet Link) que es un software mandatorio de SWIFT que se instala en los clientes. Después que el SNL es instalado y listo para su uso se pueden instalar las aplicaciones de negocios. El SNL permite el acceso del cliente a la red SWIFT a través de una ventana de acceso única y consistente, por ello garantiza la inter-operatividad entre todas las partes conectadas a la red SWIFT [2][3].

b) Network Partner

Se encarga de establecer la comunicación entre el cliente y las troncales de la red SWIFT a través de sus propias redes [3].

SWIFT solo ha autorizado a cuatro de ellos, los cuales son:

- AT&T
- BT Infonet
- Colt
- Orange Business Services

El cliente puede optar por contratar a uno o más de los network partners para la conectividad con la plataforma de SWIFT, lo que le permite la elección y la flexibilidad en el nivel de acceso a la red.

c) SWIFT

SWIFT suministra una plataforma de comunicación privada, permitiendo que los clientes puedan conectarse e intercambiar información financiera con seguridad y de forma fiable.

2.3 Conectividad a la red SWIFT

La red de SWIFT es una plataforma avanzada de mensajería, que permite a los clientes comunicar la información financiera y las transacciones de datos de forma segura y fiable.

SWIFT ofrece un amplio rango de productos de conectividad que van desde líneas basadas en internet hasta líneas de acceso permanente administrados por los network partners.

Para el acceso del cliente a la línea dedicada del network partner, SWIFT ofrece al cliente puertos de acceso con anchos de banda de 8 Kbps, 64 Kbps, 128 Kbps, 256 Kbps, 512 Kbps, T1/E1 (1536/2048 Kbps), 4 Mbps, 6 Mbps, 8 Mbps, 10 Mbps, 20 Mbps y 30 Mbps.

Los productos de conectividad a la red SWIFT son los siguientes:

a) Conectividad bronce

b) Conectividad plata

c) Conectividad oro

a) Conectividad bronce

Es un producto de conectividad de red que usa el internet para acceder a la red SWIFT. La conectividad bronce permite a los clientes establecer un canal seguro a la red SWIFT [5].

Cuando se usa el internet como medio de conexión, el cliente utiliza un router que es proporcionado por un proveedor de servicios de internet, es decir, no se emplea un network partner.

La conexión de internet no debe ser dedicado para conectarse a la red SWIFT, también puede compartirse para otros servicios de internet.

Los clientes pueden optar por conectarse por medio de la conectividad bronce de una simple conexión a internet (como se ilustra en la Figura 2.2), cuya conexión SWIFT lo soporta satisfactoriamente, donde solo una caja VPN está conectado a un router con acceso a internet.

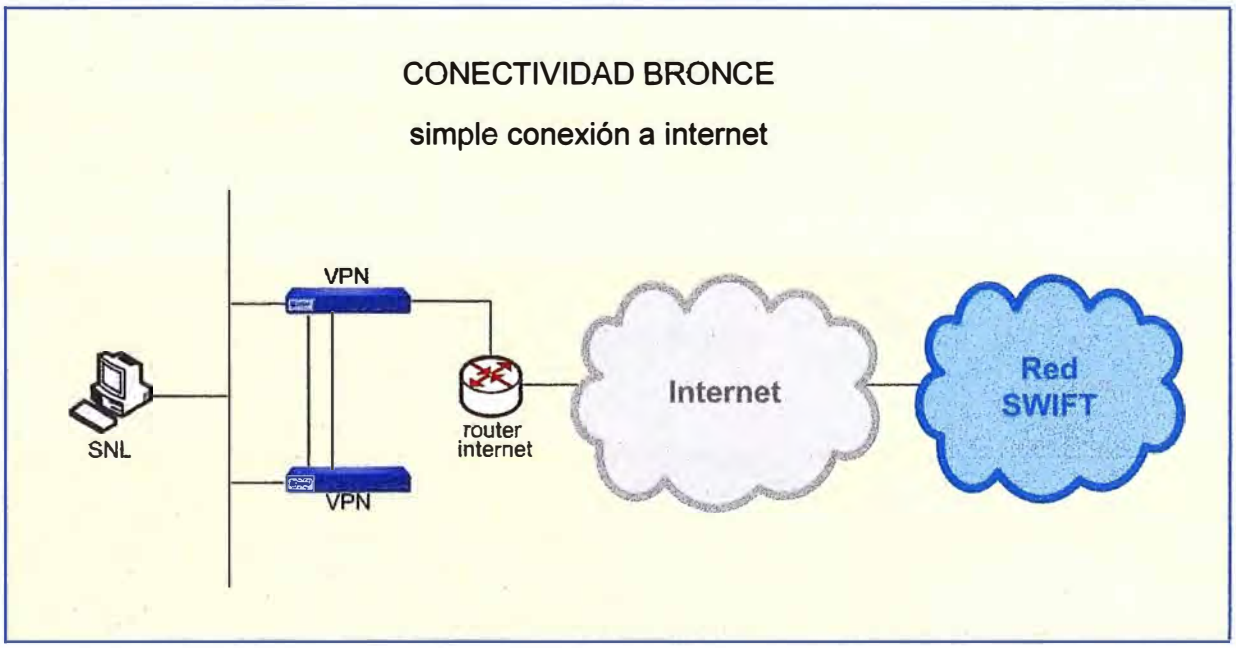

Figura 2.2 - Conectividad a la red SWIFT por medio de la conectividad bronce con una simple conexión a internet

También, los clientes pueden optar por conectarse por medio de la conectividad bronce con una doble conexión a internet (como se ilustra en la Figura 2.3), cuya conexión SWIFT lo recomienda por razones de redundancia, donde cada caja VPN está conectado a un router con acceso a internet diferente.

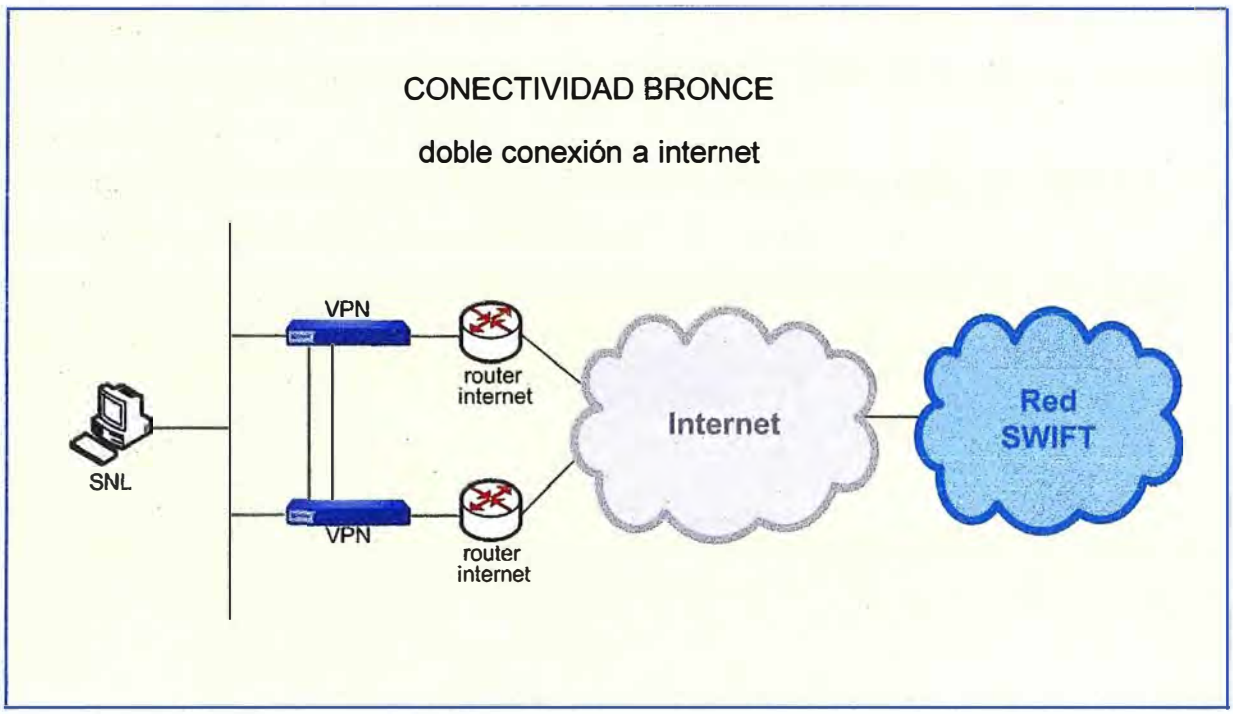

Figura 2.3 - Conectividad a la red SWIFT por medio de la conectividad bronce con una doble conexión a internet

b) Conectividad plata

Ofrece conectividad a la red SWIFT a través de una línea dedicada como canal principal y una línea de internet como canal de reserva [6].

Como se ilustra en la Figura 2.4 el network partner se encarga de establecer la línea dedicada como el canal principal.

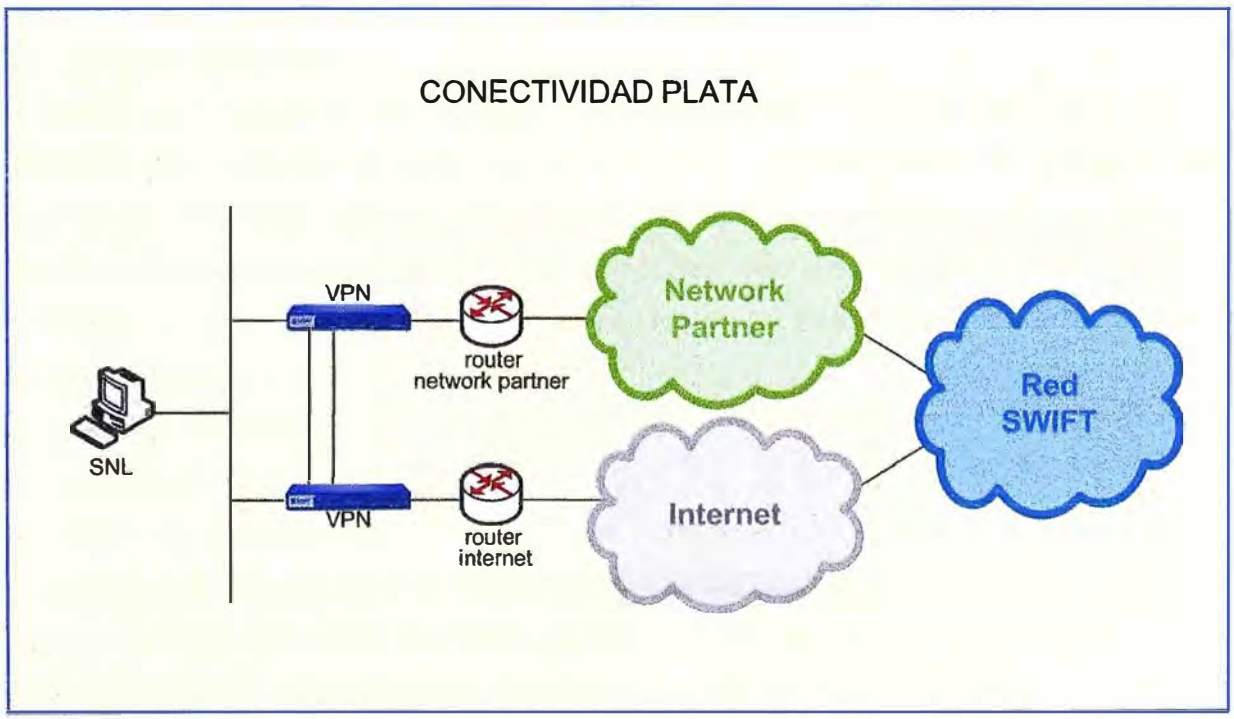

Figura 2.4 - Conectividad a la red SWIFT por medio de la conectividad plata

c) Conectividad oro

Ofrece conectividad a la red SWIFT a través de dos líneas dedicadas de la misma capacidad [7].

Como se ilustra en la Figura 2.5 las dos líneas dedicadas pueden pertenecer a dos network partners diferentes, como también a un mismo network partner.

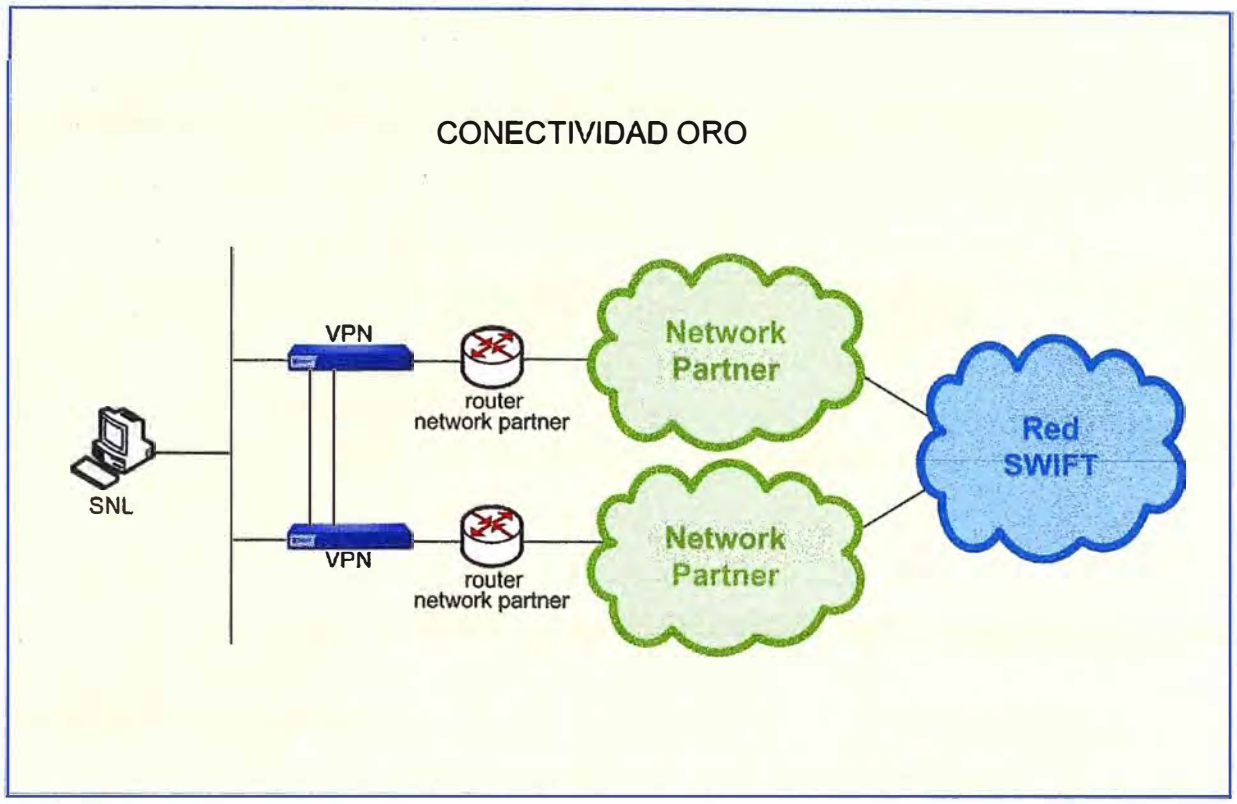

Figura 2.5 - Conectividad a la red SWIFT por medio de la conectividad oro

2.4 Mensaje financiero

SWIFT se compone de aplicaciones que realizan tareas relacionadas con el envío y recepción de mensajes a través de la red SWIFT. La elaboración de los mensajes financieros se realiza por medio de las aplicaciones instaladas en los clientes (instituciones financieras), las cuales pueden ser de forma automática o manual [13][16].

Se puede considerar una aplicación que se divide en tres etapas para la elaboración de los mensajes financieros, los cuales son:

a) Creación del mensaje
b) Aprobación del mensaje
c) Modificación del mensaje

La Figura 2.6 ilustra las tres etapas de la elaboración de un mensaje financiero, los cuales se utilizan para crear, verificar, autorizar y modificar los mensajes financieros. Una vez elegido el flujo adecuado para la elaboración del mensaje, finalmente este mensaje es enviado a la red SWIFT.

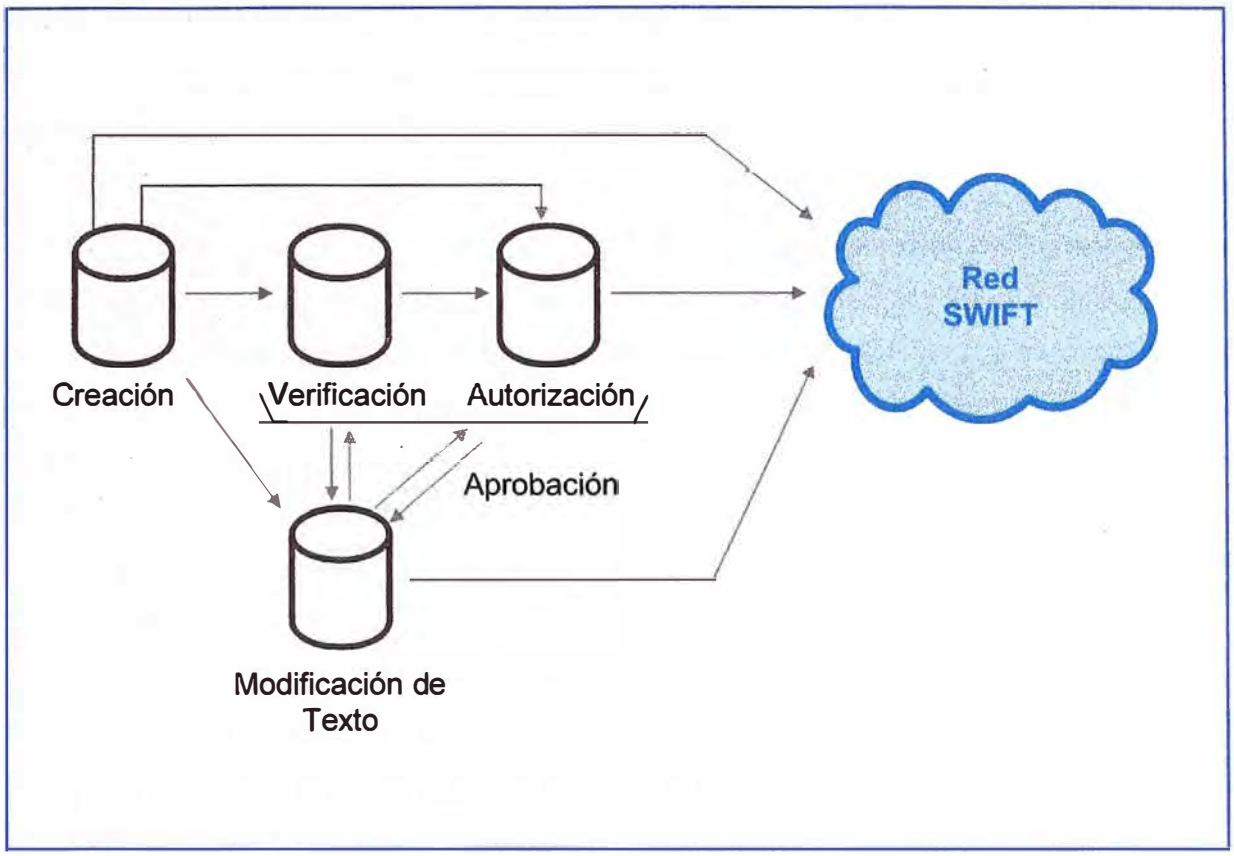

Figura 2.6 - Flujo del mensaje financiero

a) Creación del mensaje

Proporciona todas las funciones necesarias para crear los mensajes, en el cual se especifica la identidad del remitente y del receptor del mensaje, cuyo texto del mensaje es formado por el llenado de todos los campos. Después de crear el mensaje, se envía a otra cola de mensajes para que el proceso pueda continuar. Un mensaje creado suele ser enviado a la cola de verificación.

b) Aprobación del mensaje

Los mensajes generalmente deben de ser verificados o autorizados, o ambos, como una forma de aprobarse el contenido del mensaje.

Verificación

Cualquier mensaje con información importante presenta campos clave en su estructura, tales como la fecha valor, la moneda, y la cantidad. Para ello, cuando el mensaje es mostrado y aparecen los espacios en blanco el verificador reingresa los campos clave, los cuales deben coincidir con los campos que se colocaron en el momento de la creación del mensaje; de esta forma el mensaje es verificado correctamente. Después de verificar el mensaje, se envía a otra cola para que el procesamiento del mensaje pueda continuar. Un mensaje verificado suele ser enviado a la cola de autorización.

Autorización

Consiste en dar un control visual final del contenido del mensaje, para comprobar la validez de los campos y luego enviarlo a la red SWIFT.

c) Modificación del mensaje

Los mensajes que tienen un error de validación durante la creación del mensaje, o que tienen un error en la verificación o autorización, pueden ser enviados a una cola de mensajes de texto de modificación para su posterior edición. En la cola de modificación se revisa el contenido del mensaje y se realiza los cambios que sean requeridos. Luego que el mensaje es modificado se envía a la cola apropiada para que el proceso continúe.

Tipos de mensajes financieros

Existe una gran variedad de mensajes financieros, los cuales se pueden clasificar en nueve categorías [16]:

- Categoría 1: Son mensajes de pagos (transferencia de fondos) que realiza un cliente de una institución financiera a un cliente de otra institución financiera.
- Categoría 2: Son mensajes de pagos (transferencia de fondos) que se realizan entre las instituciones financieras.
- Categoría 3: Son mensajes que confirman que los pagos han sido realizados. Esta confirmación se da entre las instituciones financieras.
- Categoría 4: Son mensajes de colecciones de cartas de efectivo o cheques, el cual se da entre instituciones financieras.
- Categoría 5: Son mensajes de operaciones de valores como bonos, pagarés, acciones, certificados que se dan entre las instituciones financieras.
- Categoría 6: Son los mensajes enviados o intercambiados entre las instituciones financieras que participan en transacciones de metales preciosos.
- Categoría 7: Son mensajes que se intercambian entre las instituciones financieras que participan en el crédito documentario y la garantía de negocios.
- Categoría 8: Son mensajes que se refieren a los cheques de viaje y liquidación de ventas, reembolsos, y la administración de inventario.
- Categoría 9: Son mensajes de reporte de balance, de compensación o de estado de cuenta que se intercambian entre las instituciones financieras.

Cada categoría tiene varios tipos de mensaje (MT, por sus siglas en inglés: Message Type) que son identificados por un número de 3 dígitos, donde el primer dígito identifica la categoría. Algunos ejemplos de tipos de mensajes son:

- MT103: mensaje de transferencia de fondos de un cliente simple (Categoría 1)
- MT202: mensaje de movimiento de fondos entre instituciones financieras (Categoría 2)

- MT320: mensaje que confirma los términos de un contrato relativo a un préstamo o depósito fijo de una transacción (Categoría 3)
- MT900: mensaje de confirmación de débito (Categoría 9)
- MT910: mensaje de confirmación de crédito (Categoría 9)

2.5 Código de identificación

El código de identificación de una entidad mercantil (BIC, por sus siglas en inglés: Business Identifier Code) es el identificador internacional de instituciones financieras más utilizado. El código BIC se utiliza en las transacciones financieras, debido a que identifica a cada una de las instituciones financieras que intervienen en la transacción [15][16].

Hay dos tipos de BIC:

a) BIC de 8 caracteres
b) BIC de 11 caracteres

a) BIC de 8 caracteres

También denominado "BIC8". Un BIC8 identifica una institución financiera en un país con su respectiva ubicación, por ejemplo: BNPAFRPP

La estructura de un BIC de 8 caracteres es dado por los siguientes códigos:

Código de entidad

El código de entidad identifica la institución, el cual consta de cuatro caracteres alfabéticos, por ejemplo, BNPA (BNPAFRPP) para BNP-Paribas.

Código de país

El código de país identifica el país en el que se encuentra la institución, el cual consta de dos caracteres alfabéticos, por ejemplo, FR (BNPAFRPP) para Francia

Código de localidad

El código de localidad proporciona diferenciación geográfica dentro de un país como, por ejemplo, una ciudad, estado, provincia, el cual consta de dos caracteres que pueden ser alfabéticos o numéricos, por ejemplo, PP (BNPAFRPP) para París.

b) BIC de 11 caracteres

Opcionalmente, un BIC de 8 caracteres se puede ampliar a BIC de 11 caracteres agregándole un código de sucursal.

El código de sucursal identifica la sucursal física de una entidad, por ejemplo, MAR para Marsella, o su departamento o tipo de negocio. El código consta de tres caracteres alfanuméricos. Ejemplo: BNPAFRPP MAR

2.6 Infraestructura de clave pública de la red SWIFT

La infraestructura de clave pública de la red SWIFT (SWIFTNet PKI) registra y certifica a las instituciones financieras, para que les permita enviar y recibir mensajes a través de su red. También permite almacenar las claves públicas de todas las instituciones

financieras que forman parte de ella, garantizando que la clave pública de una institución es la correcta y no ha sido manipulado o reemplazado por un tercero [1].

La infraestructura de clave pública de la red SWIFT administra los siguientes componentes (como se ilustra en la Figura 2.7):

Autoridad de registro de la red SWIFT

Es un componente administrado por SWIFT que permite registrar a cada institución que solicita ser miembro de la red SWIFT.

Autoridad de certificación de la red SWIFT

Es un componente administrado por SWIFT que certifica que una institución ya es miembro de SWIFT.

Directorio de la red SWIFT

Es un componente administrado por SWIFT que almacena los certificados (asociado a las claves) en un directorio central.

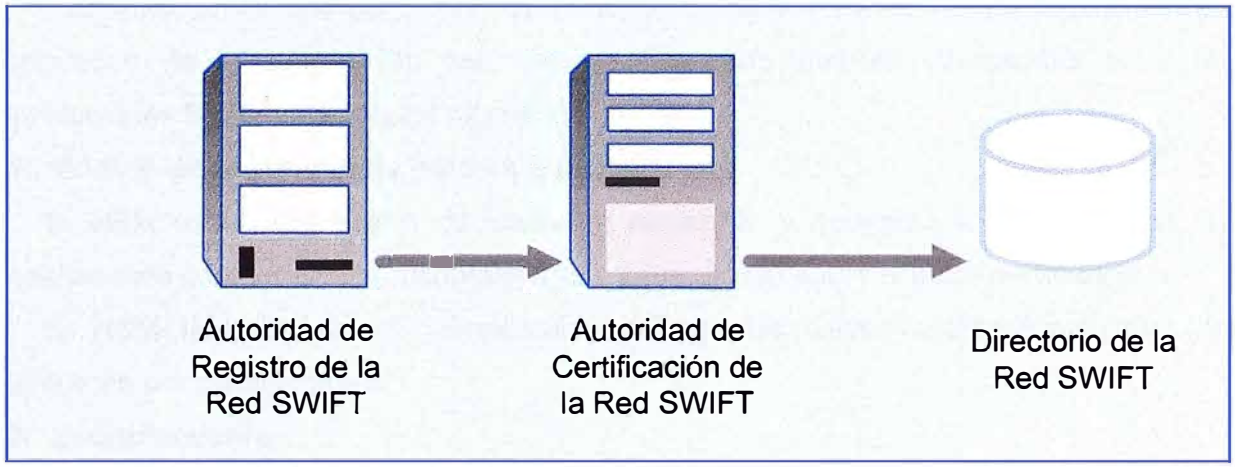

Figura 2.7 - Componentes administrados por la infraestructura de clave pública de la red SWIFT

CAPÍTULO III
METODOLOGÍA DE SOLUCIÓN

Para garantizar la seguridad de la información del mensaje financiero que se intercambia entre instituciones financieras, se tiene que mantener la confidencialidad, autenticidad, integridad y no repudio del mensaje. Para ello, en el lado del cliente del sistema de comunicaciones SWIFT se emplea un dispositivo de hardware que realizará todas las operaciones criptográficas sobre el mensaje financiero para otorgarle seguridad a su información.

Por tanto, en el lado del cliente los métodos de solución a aplicar para garantizar la seguridad de la información del mensaje financiero que se intercambia entre las instituciones financieras son los siguientes:

1. Módulo de seguridad de hardware (HSM)

El HSM es un dispositivo de hardware resistente y dedicado a realizar todas las operaciones criptográficas (encriptamiento y firma digital) sobre el mensaje financiero.

El HSM también genera, almacena y protege las claves criptográficas que son utilizadas por los algoritmos.

2. Encriptamiento

El encriptamiento mantiene la confidencialidad del mensaje financiero (usando el algoritmo asimétrico RSA y el algoritmo simétrico triple DES).

El mensaje financiero es cifrado con una clave secreta usando el algoritmo simétrico y luego la clave secreta es cifrada con la clave pública del receptor usando el algoritmo asimétrico.

3. Firma digital

La firma digital mantiene la autenticidad, integridad y no repudio del mensaje financiero (usando el algoritmo asimétrico RSA y la función hash). Al mensaje financiero se le aplica una función hash para obtener un código hash, luego este código es cifrado con la clave privada del emisor para obtener la firma.

En la Figura 3.1 se muestra como el HSM entrega las claves privadas y el directorio de la red SWIFT entrega las claves públicas para realizar todas las operaciones criptográficas sobre el mensaje financiero. Todas estas operaciones criptográficas (encriptamiento y firma digital) se realizan en el HSM [11].

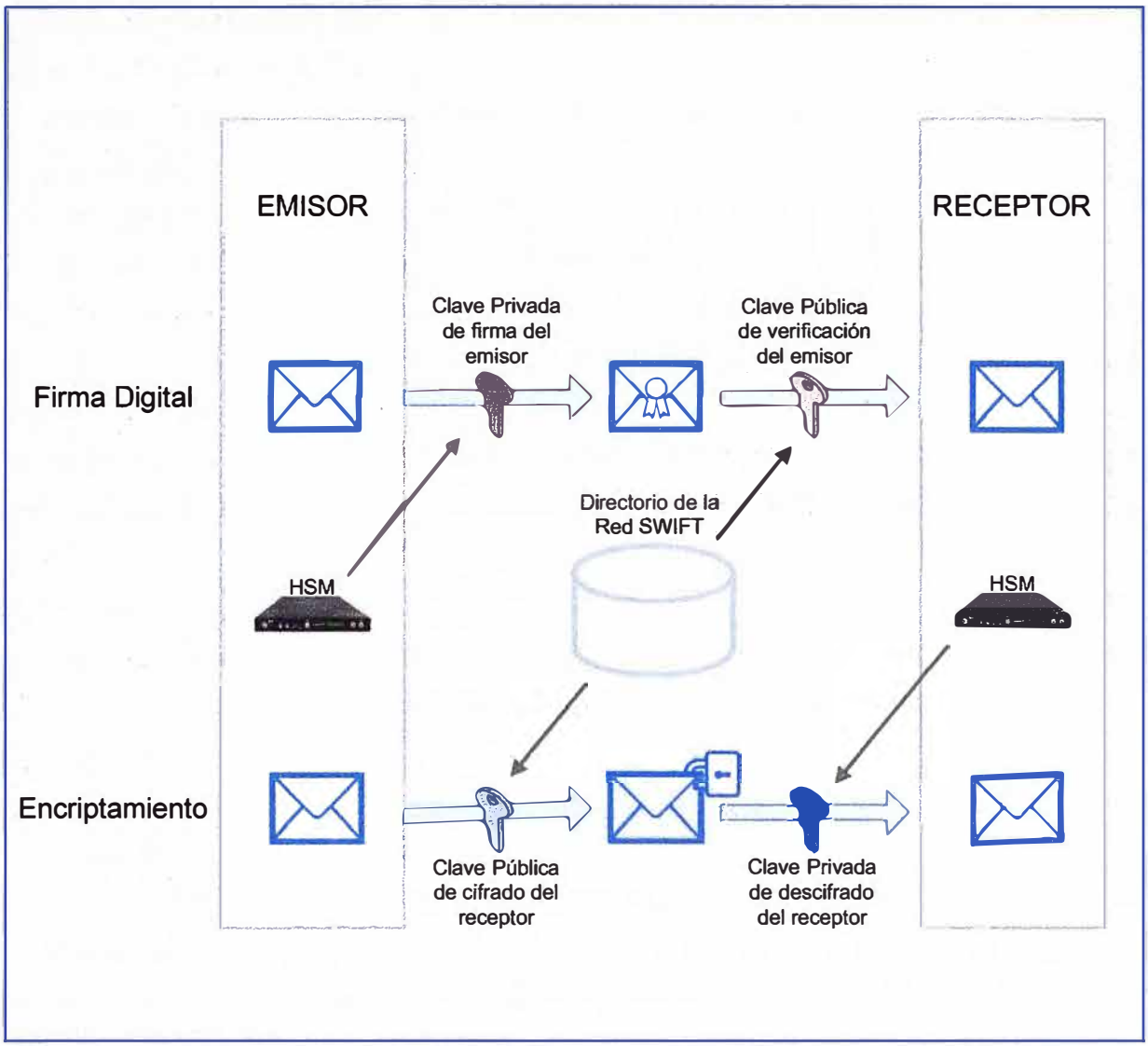

Figura 3.1 - Encriptamiento y firma digital de un mensaje financiero con el HSM

3.1 Módulo de seguridad de hardware (HSM)

El módulo de seguridad de hardware es un dispositivo de seguridad resistente que los clientes (instituciones financieras) usan para generar, almacenar y proteger las claves criptográficas, que son necesarios para las operaciones criptográficas en el entorno de la infraestructura de clave pública de la red SWIFT.

Estas operaciones criptográficas incluyen el cifrado y descifrado de un mensaje, la generación de la firma digital (el proceso de firma de un mensaje), y la verificación de la firma [2].

Todas las operaciones criptográficas se realizan dentro del HSM. El HSM protege las claves privadas al cifrarlos con una contraseña, por ello protege las operaciones de clave privada, tales como la firma y el descifrado de un mensaje; pero no protege las operaciones de clave pública, tales como, verificación de la firma y el cifrado de un mensaje.

Estas operaciones de clave pública utilizan las claves públicas que son almacenados en el directorio de la red SWIFT.

El tipo de HSM que el cliente requiere se determina por factores, tales como:

- Tipo de plataforma de hardware
- Volumen de tráfico de mensajes

Hay dos tipos de HSM que un cliente puede usar:

1. HSM basado en USB (Universal Serial Bus): para administrar un bajo volumen de tráfico de mensajes (hasta 1000 mensajes por día). Estos HSM son soportados en una plataforma Windows.
2. HSM basado en LAN (Local Area Network): para administrar un bajo, mediano y alto volumen de tráfico de mensajes. Estos HSM son soportados en las plataformas Windows y UNIX.

3.1.1 HSM basado en USB

Los HSM basados en USB se personalizan para los clientes de bajo volumen de tráfico de mensajes. Hay dos tipos de HSM basados en USB, los cuales son [2][12]:

a) Token HSM
b) Tarjeta HSM

a) Token HSM

Un token HSM es un dispositivo pequeño y ligero (como se ilustra en la Figura 3.2) que se conecta a la PC del cliente (plataforma Windows) a través de un puerto USB.

La PC del cliente soporta la conexión simultánea de hasta cuatro tokens HSM. Cada token HSM almacena un único certificado y puede manejar un rendimiento limitado (hasta 1000 mensajes por día) [2].

Características técnicas de un token HSM

- Token HSM: fabricante SafeNet, modelo iKey 2032
- Conectividad: compatible con USB 1.1 y 2.0
- Velocidad de transferencia: 1.5 Mbps
- Hardware del sistema: procesador de 8 bit y memoria de 32 KB
- Dimensiones: 15.875 mm x 57.15 mm x 7.9375 mm
- Normas de certificación de regulación: FCC clase B parte 15, FIPS 140-1 nivel 2 y compatible con RoHS [4]

Figura 3.2 - Token HSM (SafeNet, iKey 2032)

b) Tarjeta HSM

La tarjeta HSM es una tarjeta de circuito impreso (como se ilustra en la Figura 3.4) que se inserta en un lector de tarjetas (como se ilustra en la Figura 3.3), que a su vez está conectado a la PC del cliente (plataforma Windows) a través de un puerto USB.

Un lector de tarjeta HSM es un dispositivo que lee información desde una tarjeta HSM y escribe información en una tarjeta HSM.

Una tarjeta HSM se asemeja a una tarjeta de crédito, y el usuario lo inserta en un lector de tarjeta HSM para realizar operaciones de claves privadas.

La PC del cliente soporta la conexión simultánea de hasta cuatro lectores de tarjetas HSM. Cada tarjeta HSM almacena un único certificado. Cada lector de tarjeta HSM puede manejar un rendimiento limitado (hasta 1000 mensajes por día) [2].

Características técnicas de un lector de tarjeta HSM y de una tarjeta HSM

- Lector de tarjeta HSM: fabricante Axalto, modelo Reflex 510
- Dimensiones: 10 mm x 70 mm x 70 mm
- Fuente de alimentación: 5 V. a través de un bus USB
- Cable: 1.5 metros de longitud con conector USB
- Conectividad: USB 2.0
- Velocidad de transferencia: 12 Mbps con la PC y 344105 bps con la tarjeta HSM
- Temperatura: de 0°C a 50°C encendido
- Conector de la tarjeta HSM: conector de 8 contactos
- Tarjeta HSM: fabricante Axalto, modelo Cyberflex Access 64 K versión 2
- Normas de certificación de regulación: FCC clase B parte 15 y FIPS 140-2 nivel 2 (tarjeta HSM) [4]

Figura 3.3 - Lector de Tarjeta HSM (Axalto, Reflex)

Figura 3.4 - Tarjeta HSM (Axalto, Cyberflex)

Características de los HSM basados en USB

Los HSM basados en USB tienen las siguientes características [2]:

- Cada tarjeta HSM o token HSM almacena un único certificado.
- Un máximo de cuatro HSM basados en USB pueden estar activos al mismo tiempo sobre una PC del cliente.
- Encajan en entornos que esperan un bajo volumen de tráfico de mensajes, es decir, hasta 1000 transacciones por día.
- Las claves se generan en la tarjeta o en el token, lo que significa que la información crítica de la clave privada nunca sale de la tarjeta o el token, y por ello no se puede extraer desde la red o desde la PC del cliente.
- Tienen protección de hardware y software en contra de ataques externos.

Ventajas de los HSM basados en USB

Las principales ventajas de HSM basados en USB son [2]:

- Facilidad de uso del HSM, donde sólo se tiene que enchufar el token HSM o el lector de tarjetas HSM en el puerto USB de la PC del cliente e insertar la tarjeta HSM en el lector.
- Portabilidad del HSM, donde los tokens y los lectores de tarjetas HSM se quitan fácilmente de la PC del cliente cuando no se necesitan. Asimismo, pueden trasladarse a otra PC con total seguridad, ya que se requiere una contraseña para acceder a los certificados.

3.1.2 HSM basado en LAN

La solución de un HSM basado en LAN es una caja HSM.

Caja HSM

La caja HSM es un dispositivo de hardware (como se ilustra en la Figura 3.5) al que se accede a través de la LAN. La caja HSM es soportada en una plataforma Windows y UNIX. Estos dispositivos pueden compartirse en red y ofrecen escalabilidad y redundancia. Cada caja HSM puede almacenar múltiples certificados [2][12].

Las cajas HSM permiten administrar un flujo de mensajes de bajo, mediano y alto tráfico, por ello, para satisfacer las necesidades de los clientes existen tres niveles de rendimiento:

- Caja HSM de bajo rendimiento: soporta hasta 10000 mensajes por día
- Caja HSM de mediano rendimiento: soporta hasta 50000 mensajes por día
- Caja HSM de alto rendimiento: soporta hasta 400000 mensajes por día

Características técnicas de una caja HSM:

- Caja HSM: fabricante SafeNet, modelo Luna Identity Server (Luna IS)
- Software: firmware y software son instalados de fábrica sobre la caja HSM. Linux es el sistema operativo.
- Fuente de alimentación: es de detección automática de 100 a 240 V. y de 50 a 60 Hz
- Ethernet: tiene dos puertos Ethernet de detección automática entre 10BaseT y 100BaseT
- Puerto serial: puerto serial macho DB9 (RS232 de 9 pines), trabaja con velocidad de 9600 bps. También viene un cable serial DB9 hembra a DB9 hembra
- PIN Entry Device (fabricante SafeNet, modelo Luna PED versión 2): es un dispositivo desmontable con pantalla LCD, teclado numérico y un slot para insertar las llaves PED
- Llaves PED: fabricante SafeNet, modelo iKey 1000. 10 tokens por cada caja HSM
- Consumo de energía: potencia a plena carga < 170 Watts
- Dimensiones: 482.6 mm x 523.2 mm x 43.9 mm
- Temperatura: de 0°C a 35°C encendido y de -20°C a 50°C apagado
- Peso: de 10 a 10.5 Kg
- Normas de certificación de regulación: FCC clase B sub-parte B parte 15, FIPS 140-2 nivel 3 y compatible con RoHS [4]

Figura 3.5 - Caja HSM (SafeNet, Luna Identity Server)

Características de las cajas HSM

Las cajas HSM tienen las siguientes características [2]:

- Almacenan hasta 250 certificados.
- Se puede hacer un clúster de dos cajas HSM, que es una configuración altamente resistente.
- Tiene tres niveles de rendimiento (bajo, medio y alto). Por lo tanto, se adaptan a entornos que esperan un volumen de tráfico de bajo a alto.

Ventajas de las cajas HSM

Las principales ventajas de las cajas HSM son [2]:

- Se comparten en una red; donde las cajas HSM son accesibles a través de la LAN.
- Escalabilidad; es decir las cajas HSM tienen capacidad para almacenar centenares de certificados y admiten un caudal de bajo a alto.
- Redundancia; donde las cajas HSM pueden configurarse en un clúster de dos cajas HSM para disminuir al mínimo el tiempo de inactividad y proteger los certificados en caso falle una caja HSM. Las cajas poseen los mismos certificados y controlan el tráfico en paralelo.

Acceso seguro a una caja HSM

Cada caja HSM se suministra con un PED, varias llaves PED y con los cables de conexión y alimentación necesarios, los cuales pueden ser montados en un rack [2][12].

El acceso seguro a una caja HSM es proporcionado por:

a) El PED

b) Las llaves PED

c) Los códigos PIN de las llaves PED

a) PED

Un PED (PIN Entry Device) se suministra con cada caja HSM. Un PED es un dispositivo portátil que comprende un teclado numérico y una pantalla LCD (como se ilustra en la Figura 3.6), y se conecta a la caja HSM con un cable (como se ilustra en la Figura 3.7). El PED permite controlar el acceso a la caja HSM [2][12].

Después que el PED se enciende, muestra el mensaje: “a la espera de comandos”, luego recibe una instrucción de trabajo de la caja HSM, que le pide información o le indica que debe realizar una acción relacionada con la instrucción. Típicamente, una tarea puede requerir una serie de instrucciones para obtener información y tomar acciones.

Por ejemplo, una tarea puede requerir una respuesta a una pregunta, introducir una llave PED, seguido por un código PIN, y luego una respuesta a una segunda pregunta. La respuesta a la segunda pregunta puede generar otra tarea con una serie de preguntas, y así sucesivamente.

Figura 3.6 - PED (SafeNet, Luna PED)

Figura 3.7 - PED conectado a la caja HSM

b) Llaves PED

Las llaves PED son tokens USB que se utilizan para la autenticación de las operaciones PED (como se ilustra en la Figura 3.8).

Una llave PED se conecta al puerto USB de la parte superior de un PED y se introduce un código PIN para continuar utilizando el PED [2][12].

Las llaves PED se inicializan durante la instalación de una caja HSM primaria, y se asignan funciones diferentes. Las llaves PED se utilizan para la autenticación de cierta configuración, gestión y tareas administrativas que se realizan en la caja HSM.

Las llaves PED almacenan datos de forma segura y proporcionan autenticación adicional para el ejercicio de funciones administrativas en las cajas HSM.

Durante la configuración de las cajas HSM primarias, la data se almacena de forma segura en las llaves, y los códigos PIN se asignan a cada llave PED. La data segura se utiliza para configurar una segunda caja HSM.

Figura 3.8 - Llave PED (SafeNet, iKey 1000)

Los tipos de llaves PED son:

- Llave SO: permite realizar funciones administrativas en las cajas HSM, para ello se debe ingresar con una cuenta admin o recover en la caja HSM.

- Llave Domain: al agregar una segunda caja HSM, se debe utilizar la llave Domain que fue inicializada en la caja HSM primaria del clúster. Esto asegura que los certificados se replican correctamente desde la caja HSM primaria a la secundaria.
- Llave User: permite que todas las particiones de la caja HSM que contienen los certificados individuales sean agrupados en una simple entidad.

Los duplicados de las llaves PED se pueden crear durante el procedimiento de instalación de la caja HSM, de modo que se tiene por lo menos dos llaves PED inicializados de cada tipo.

Se tienen que almacenar las llaves PED (y las llaves duplicadas) de forma segura, ya que proporcionan acceso a la caja HSM, donde los duplicados de las llaves pueden ser utilizados si el grupo principal de llaves llegan a perderse o a ser dañados.

c) Los códigos PIN de las llaves PED

El código PIN para una llave PED debe contener entre 4 y 8 dígitos. El código PIN se utiliza para desbloquear el secreto de la llave para que pueda ser utilizado por una operación PED con una caja HSM. El código PIN se almacena en la llave y no se pasa a la caja HSM [2][12].

El duplicado de una llave puede tener el mismo código PIN que la llave original del mismo tipo, o puede tener diferente código PIN. Si el mismo código PIN se utiliza para todas las llaves duplicadas del mismo tipo, las llaves son intercambiables.

Clúster HSM

Un clúster es una agrupación de dos cajas HSM. Con el suministro de las dos cajas HSM, la implementación estándar de estas cajas es conectarlos y configurarlos en la red como un clúster. Los beneficios de un clúster son evitar tiempos muertos y evitar la necesidad de recuperar los certificados en caso una caja falle [2].

Cada caja HSM en un clúster es configurado con una dirección IP. Además, cada caja HSM pertenece al mismo dominio, que asegura que los certificados se replican de forma segura entre las cajas. Las cajas HSM en un clúster forman una unidad operacional, y son usados igualmente para firmar mensajes. Sin embargo, tienen funciones diferentes (primaria o secundaria) para las operaciones de administración de los certificados.

La función de las cajas HSM es determinada por el orden en el cual son instaladas. Una sola caja HSM es siempre la caja HSM primaria. Si se agrega una segunda caja HSM, se convierte en la caja HSM secundaria. Cuando se agrega una nueva caja HSM a un clúster, la caja HSM primaria replica los certificados a la nueva caja. Una sola caja HSM no proporciona alta disponibilidad ya que los certificados se pierden si la caja HSM falla. Un clúster con dos cajas HSM ofrece una alta disponibilidad.

La disponibilidad de las cajas HSM se encuentra dado por las siguientes configuraciones [2]:

a) Configuración de alta disponibilidad

b) Configuración de baja disponibilidad

a) Configuración de alta disponibilidad

Una configuración de dos cajas HSM por clúster proporciona un entorno de alta disponibilidad para el uso de los certificados.

La Figura 3.9 ilustra una configuración de alta disponibilidad de cuatro cajas HSM, donde se forma dos clúster de dos cajas HSM cada uno.

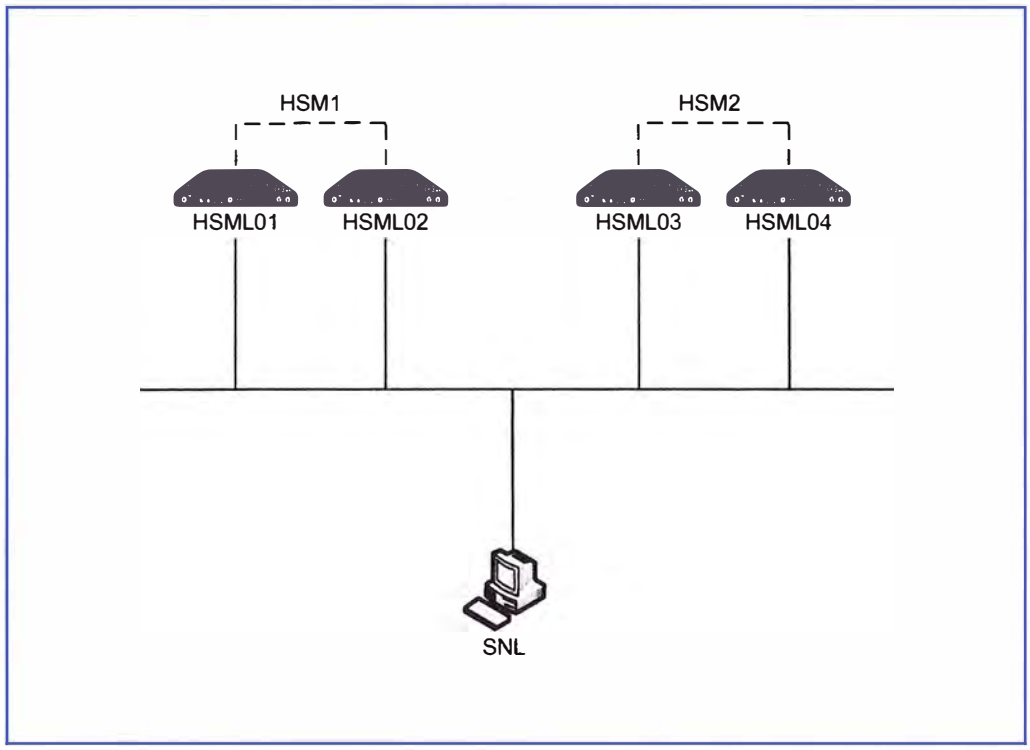

Figura 3.9 - Configuración de alta disponibilidad de las cajas HSM

Donde:

- HSM1 y HSM2 son los clúster HSM
- HSML01 es la caja HSM Primaria en el clúster HSM1
- HSML02 es la caja HSM Secundaria en el clúster HSM1

HSML03 es la caja HSM Primaria en el clúster HSM2

- HSML04 es la caja HSM Secundaria en el clúster HSM2

b) Configuración de baja disponibilidad

Una configuración de dos cajas HSM de manera independiente proporciona un entorno de baja disponibilidad. Un entorno de baja disponibilidad puede dar lugar a la pérdida de los certificados que se almacenan en una caja HSM. Esta configuración se utiliza sólo en un entorno de prueba, donde el tiempo de inactividad no es crítico. Por ello,

no es recomendable tener una sola caja HSM debido a que solo tendría una configuración de baja disponibilidad.

La Figura 3.10 ilustra una configuración de baja disponibilidad de las dos cajas HSM, las cuales no están en clúster sino cada una de forma independiente.

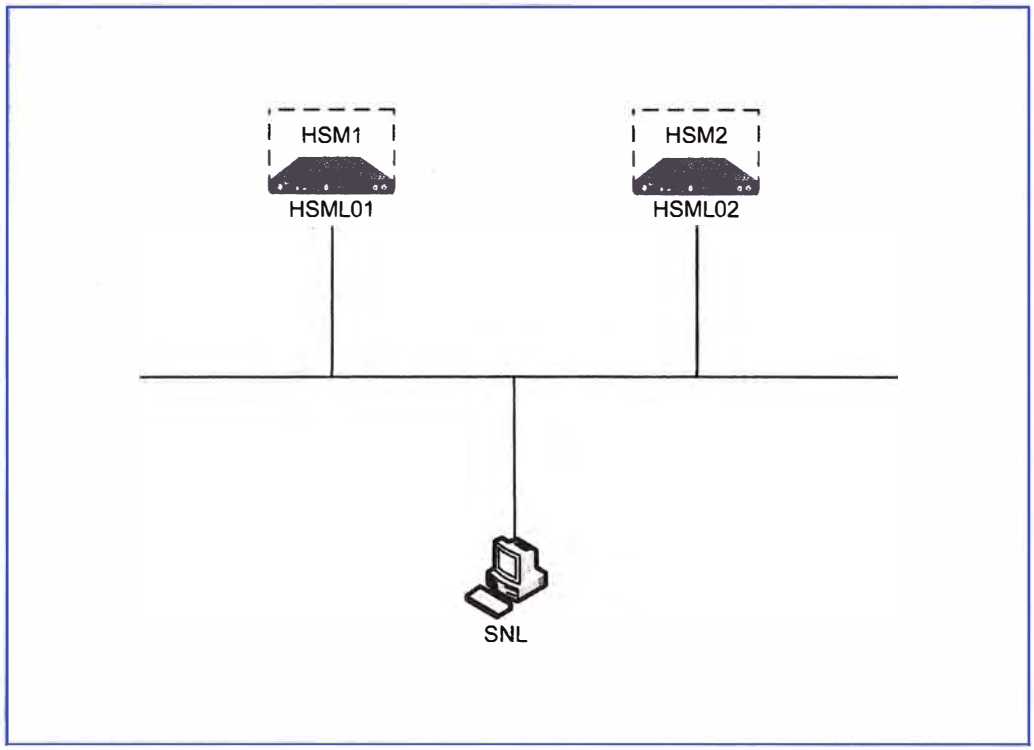

Figura 3.10 - Configuración de baja disponibilidad de las cajas HSM

Donde:

- HSM1 y HSM2 son los clúster HSM
- HSML01 es la única caja HSM en el clúster HSM1
- HSML02 es la única caja HSM en el clúster HSM2

Cuentas de usuario de las cajas HSM

Los roles de un usuario pueden ser asignados a las cuentas de usuario para controlar los tipos de tareas que el usuario puede realizar, tales como, administrar, operar, o monitorizar la caja HSM [2].

La caja HSM tiene los siguientes tipos de roles de usuario:

a) admin
b) operator
c) monitor
d) recover

a) Cuenta admin

Los usuarios con este rol pueden realizar tareas, tales como, desbloquear un certificado, inicializar una partición, y de instalar o actualizar el software de HSM. El

usuario admin puede garantizar la seguridad de las llaves PED, y la administración de la caja HSM.

b) Cuenta operator

Los usuarios con este rol pueden realizar tareas a nivel de sistema, tales como, la activación y desactivación de una partición, y reinicio de una caja HSM.

c) Cuenta monitor

La cuenta monitor es utilizada para monitorear el estado y condición de las cajas HSM.

d) Cuenta recover

Los usuarios con este rol pueden conectarse a una caja HSM a través del único puerto serial, y con una aplicación, tal como, el HyperTerminal. Este rol se utiliza para reiniciar la cuenta admin (si está bloqueado), y para reiniciar una caja HSM a su configuración predeterminada de fábrica. La cuenta recover no puede ser bloqueada. Está protegido por la llave SO y su código PIN.

3.2 Encriptamiento

El encriptamiento se emplea para garantizar la confidencialidad del mensaje financiero que se envía a través de la red SWIFT, nadie salvo el destinatario puede descifrarlo [9][11].

En el lado del emisor, éste usa la clave pública del receptor (disponible para todos los clientes de la red SWIFT) para cifrar el mensaje, una vez cifrado, sólo la clave privada del receptor podrá descifrar este mensaje, ya que es el único que la conoce.

En el lado del receptor, los datos se descifran con la clave privada del receptor. Puesto que sólo la clave privada del receptor es capaz de descifrar los datos y como esta clave sólo está disponible para el receptor, el receptor tiene la seguridad de la estricta confidencialidad de la información durante su intercambio.

En la Figura 3.11, se muestra la secuencia de encriptamiento que tiene un mensaje financiero, el cual emplea una criptografía híbrida debido a que usa tanto un cifrado simétrico como un cifrado asimétrico [11].

En el lado del emisor, un mensaje es cifrado simétricamente con una clave simétrica aleatoria y secreta (usando el algoritmo simétrico triple DES), y a la vez ésta clave simétrica es cifrada asimétricamente con la clave pública del receptor (usando el algoritmo asimétrico RSA), luego ambos de forma conjunta son enviados a través de la red SWIFT al receptor.

En el lado del receptor, la clave simétrica cifrada se descifra con la clave privada del receptor (usando el algoritmo asimétrico RSA), luego el mensaje es descifrado rápidamente con la clave simétrica ya descifrada (usando el algoritmo simétrico triple DES).

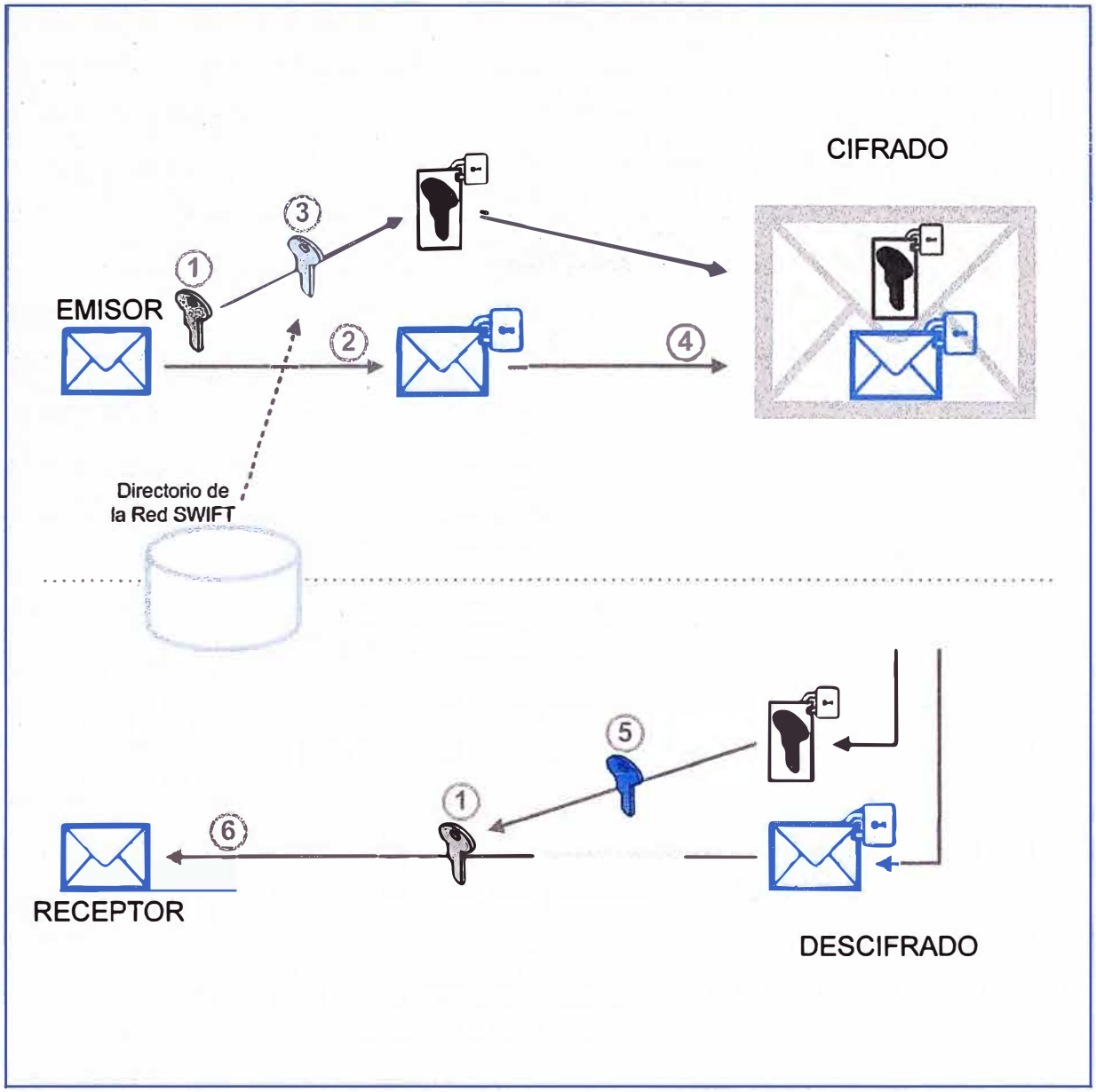

Figura 3.11 - Cifrado y descifrado de un mensaje financiero

De la Figura 3.11, el cifrado y descifrado de un mensaje financiero se indica en mayor detalle en la siguiente secuencia numérica [11]:

1. Clave secreta simétrica (clave de sesión aleatoria)
2. Mensaje es cifrado con la clave secreta (usando algoritmo simétrico triple DES)
3. Clave secreta es cifrada con la clave pública del receptor (usando algoritmo asimétrico RSA)
4. Ambos, mensaje cifrado y clave secreta cifrada son enviados al receptor
5. Clave secreta es descifrada con la clave privada del receptor (usando algoritmo asimétrico RSA)
6. Mensaje es descifrado con la clave secreta (usando algoritmo simétrico triple DES)

En la infraestructura de claves públicas de la red SWIFT, el encriptamiento de un mensaje financiero emplea los siguientes algoritmos:

- Algoritmo RSA (2048 bits) para la pareja de claves de encripción asimétrica
- Algoritmo triple DES (112 bits) para la clave de encripción simétrica

3.2.1 Algoritmo asimétrico RSA

El algoritmo RSA es un algoritmo asimétrico, por ello se procede a explicar lo siguiente:

a) Criptografía asimétrica

b) Algoritmo RSA

a) Criptografía asimétrica

La criptografía asimétrica es el método criptográfico que usa un par de claves para el envío de mensajes. Las dos claves pertenecen a la misma entidad, donde una clave es pública y se entrega a un centro de infraestructura de claves públicas, la otra clave es privada y el propietario debe guardarla de modo seguro.

Además, los métodos criptográficos garantizan que esa pareja de claves sólo se pueden generar una vez, de modo que no es posible que dos entidades hayan obtenido la misma pareja de claves [9].

Los sistemas de cifrado de clave pública o sistemas de cifrado asimétricos se inventaron con el fin de evitar por completo el problema del intercambio de claves de los sistemas de cifrado simétricos.

Con las claves públicas no es necesario que el remitente y el destinatario se pongan de acuerdo en la clave a emplear. Todo lo que se requiere es que, antes de iniciar la comunicación secreta, el remitente consiga una copia de la clave pública del destinatario. Es más, esa misma clave pública puede ser usada por cualquiera que desee comunicarse con su propietario.

Como con los sistemas de cifrado simétricos buenos, con un buen sistema de cifrado de clave pública toda la seguridad descansa en la clave y no en el algoritmo. Por lo tanto, el tamaño de la clave es una medida de la seguridad del sistema.

La mayor ventaja de la criptografía asimétrica es que se puede cifrar con una clave y descifrar con la otra, pero este sistema tiene las siguientes desventajas:

- Para una misma longitud de clave y mensaje se necesita mayor tiempo de proceso.
- Las claves deben ser de mayor tamaño que las simétricas.
- El mensaje cifrado ocupa más espacio que el original.

La Figura 3.12 ilustra una clave pública para cifrar el mensaje y una clave privada para descifrarlo, es decir se usan un par de claves diferentes pero relacionadas.

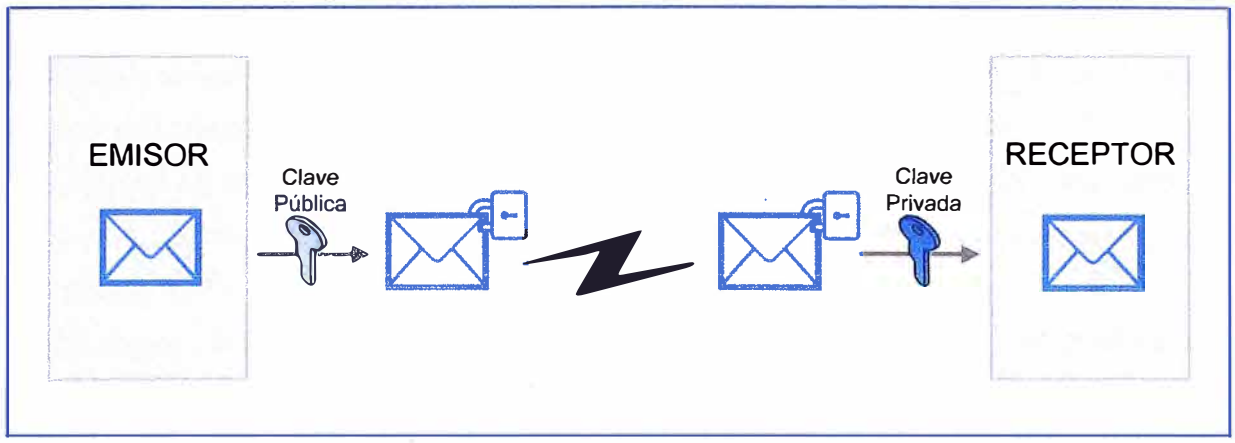

Figura 3.12 - Clave pública y privada en una criptografía asimétrica

b) Algoritmo RSA

En criptografía, RSA (el nombre se debe a sus tres inventores: Rivest, Shamir y Adleman) es un sistema criptográfico de clave pública que apareció en 1977. En la actualidad, RSA es el primer y más utilizado algoritmo de este tipo. En muchos de los algoritmos asimétricos ambas claves sirven tanto para cifrar como para descifrar, de manera que si se emplea una para codificar, la otra permitiría decodificar y viceversa [9][10].

La seguridad de este algoritmo se basa en la dificultad de la factorización de grandes números enteros. Las claves pública y privada se calculan a partir de un número que se obtiene como producto de dos números primos grandes (números primos mantenidos en secreto). El descomponer un número relativamente grande resulta muy difícil y en algunos casos casi imposible. Sin embargo, el caso inverso consistente en dados los factores primos hallar el número, es sencillo, solo se requiere multiplicar los factores. Por ello, generar números primos requiere mucho tiempo, descomponer números en factores primos requiere un poco más de tiempo, pero construir un número a partir de sus factores primos es rápido. RSA se mantendrá seguro mientras no se conozcan formas rápidas de descomponer un número grande en producto de números primos.

Funcionamiento del algoritmo RSA

Cuando el emisor E manda un mensaje encriptado al receptor R no puede estar seguro de que el canal no sea espiado, por ello su objetivo es que este mensaje encriptado aunque sea interceptado, no pueda ser descifrado y por tanto entendido. Los pasos a seguir para que el mensaje sea encriptado por medio del algoritmo RSA son los siguientes:

- En privado, el receptor R escoge dos números primos p y q muy grandes (de por lo menos 100 cifras cada uno), y los multiplica, obteniendo $n = pq$ (donde n tiene que ser

difícil de factorizar). Por motivos de seguridad, estos números deben escogerse de forma aleatoria y también deben de tener una longitud en bits similar. Se pueden hallar números primos fácilmente mediante un test de primalidad.

- También en privado, el receptor R obtiene el valor de la función $\varphi(n)$, que como se sabe en este caso será igual a $\varphi(n) = \varphi(pq) = \varphi(p)\varphi(q) = (p - 1)(q - 1)$, dado que p y q son primos entre sí, y cada uno de ellos es primo.
- En privado, el receptor R escoge un número e tal que $1 < e < \varphi(n)$ de manera que sea primo relativo con $\varphi(n)$. Donde e es conocido como el exponente de la clave pública.
- Se determina un d que satisfaga la congruencia $d = e^{-1} \bmod \varphi(n)$, es decir que d es el multiplicador modular inverso de e módulo $\varphi(n)$. Donde d es conocido como el exponente de la clave privada.
- El receptor R guarda en secreto el par de números (d, n), lo cual es llamado la clave privada, que utilizará para descifrar los mensajes que le envíen (en realidad solo va a utilizar el número d).
- El receptor R hace público el par de números (e, n), lo cual es llamado la clave pública, que los demás usuarios utilizarán para cifrar los mensajes.
- El emisor E, que desea enviar un mensaje confidencial m al receptor R, lo encripta del siguiente modo: $c = m^e \pmod n$, cosa que puede hacer debido a que conoce los números e y n que R hizo públicos. Luego de calculado el mensaje cifrado c, éste se envía.
- El receptor R recibe el mensaje cifrado c y ejecuta con él la siguiente operación: $m=c^d \pmod n$, cosa que puede hacer debido a que conoce el valor de su propia clave privada, d. El procedimiento anterior funciona porque: $c^d=(m^e)^d=m^{ed}=m$, puesto que d y e eran inversos en módulo $\varphi(n)$. En resumen, receptor R puede conocer el mensaje m que el emisor E le envió.

Teniendo en cuenta los avances de la tecnología, y suponiendo que el algoritmo RSA no sea roto analíticamente, se debe escoger la longitud de la clave en función del tiempo que se quiera que la información permanezca en secreto. Efectivamente, una clave de 1024 bits parece demasiado corta como para proteger información por más de unos pocos años. Por ello, una clave tiene que ser renovada periódicamente.

3.2.2 Algoritmo simétrico triple DES

El algoritmo triple DES es un algoritmo simétrico que utiliza el algoritmo DES tres veces, por ello se procede a explicar lo siguiente:

a) Criptografía simétrica

b) Algoritmo DES

c) Algoritmo triple DES

a) Criptografía simétrica

La criptografía simétrica es un método criptográfico en el cual se usa una misma clave para cifrar y descifrar mensajes. Las dos partes que se comunican han de ponerse de acuerdo de antemano sobre la clave a usar. Una vez ambas tienen acceso a esta clave, el remitente cifra un mensaje usándola, lo envía al destinatario, y éste lo descifra con la misma [9].

Un buen sistema de cifrado pone toda la seguridad en la clave y ninguna en el algoritmo. En otras palabras, no debería ser de ninguna ayuda para un atacante conocer el algoritmo que se está usando. Sólo si el atacante obtuviera la clave, le serviría conocer el algoritmo. Dado que toda la seguridad está en la clave, es importante que sea muy difícil adivinar el tipo de clave. Esto quiere decir que el abanico de claves posibles, o sea, el espacio de posibilidades de claves, debe ser amplio.

La Figura 3.13 ilustra una criptografía simétrica, donde se usa una clave simétrica para cifrar un mensaje, luego lo envía y el destinatario lo descifra usando la misma clave simétrica.

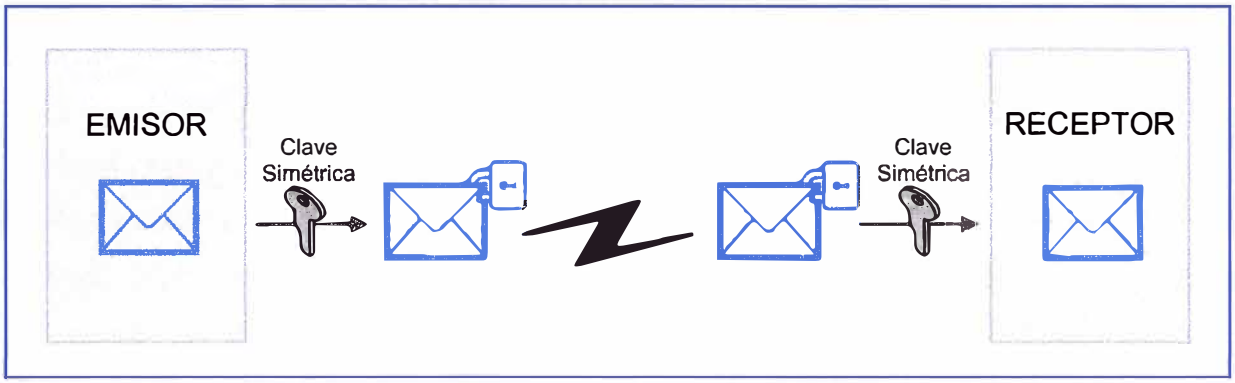

Figura 3.13 - Clave simétrica común en una criptografía simétrica

b) Algoritmo DES

Data Encryption Standard (DES) es un algoritmo desarrollado originalmente por IBM y posteriormente fue modificado y adoptado por el gobierno de Estados Unidos en 1977 como estándar de cifrado de todas las informaciones.

DES es un algoritmo de cifrado por bloques. El tamaño del bloque es de 64 bits (8 bytes). La clave efectiva de DES es de 56 bits, el cual se obtiene de una clave de entrada de 64 bits, donde 8 bits se usan únicamente para comprobar la paridad y luego son descartados, por ello los 56 restantes son empleados por el algoritmo [9][10].

Actualmente DES se considera inseguro para muchas aplicaciones, debido principalmente a que el tamaño de la clave de 56 bits es corto. Este algoritmo es más seguro en su variante de triple DES.

Funcionamiento del algoritmo DES

El funcionamiento del algoritmo DES está basado en los criptosistemas de Feistel, el cual consiste en realizar siempre las mismas operaciones un número determinado de veces, en este caso 16 veces.

Los pasos a seguir para que el mensaje sea encriptado por medio del algoritmo DES son los siguientes:

- El bloque de datos de 64 bits se divide en 2 partes de 32 bits, los cuales son la parte derecha y la parte izquierda (estas partes son procesados de forma alternada).
- Se toma una función F y una sub clave K_i
- Se realizan una serie de operaciones complejas con F y K_i a la parte derecha (esta operación se realiza 16 veces).
- Se suma la parte izquierda con el resultado de la operación compleja que se realizó con F y K_i a la parte derecha.
- Se intercambian la parte izquierda con la parte derecha, siendo ahora la parte izquierda el resultado de la operación de la parte derecha.
- Estas operaciones se repitan 16 veces, y en la operación 16 ya no se realiza el intercambio de las partes.
- La operación de descifrado es exactamente la misma de cifrado, pero en este caso se toman las sub claves en orden inverso de K_{16} a K_1.

c) Algoritmo triple DES

Triple DES es una modalidad más avanzada de DES, debido a que usa el algoritmo tres veces. Triple DES es conocido también como 3DES o TDES, fue desarrollado por IBM en 1998 [9][10].

El algoritmo triple DES tiene dos variantes:

- Triple DES con dos claves, consiste en una triple encriptación DES con dos claves, donde la primera y tercera clave son iguales. En este caso la clave resultante es de 112 bits.
- Triple DES con tres claves, consiste en una triple encriptación DES con tres claves, donde las tres claves son diferentes. En este caso la clave resultante es de 168 bits.

Cuando con el DES la clave de 56 bits no era suficiente para evitar un ataque informático, el triple DES fue elegido para agrandar el largo de la clave sin necesidad de cambiar de algoritmo de cifrado.

Tomando el caso de que se duplique la longitud efectiva de la clave (112 bits), igual se procede a triplicar el número de operaciones de cifrado, haciendo de este método de cifrado mucho más seguro que el DES.

3.3 Firma digital

La firma digital se emplea para garantizar la autenticidad, integridad y no repudio del mensaje financiero que se envía a través de la red SWIFT [11].

Si el propietario del par de claves usa su clave privada para cifrar el mensaje, cualquiera puede descifrarlo utilizando su clave pública. En este caso se consigue por tanto la identificación y autentificación del emisor, debido a que el propietario es el único que emplea su clave privada. Esta idea es el fundamento de la firma digital [9].

En la Figura 3.14 ilustra el proceso de la firma digital en el lado del emisor y el proceso de verificación de la firma en el lado del receptor [11].

En el lado del emisor, se ejecuta una función hash al mensaje obteniéndose un código hash, cuyo código es cifrado asimétricamente con la clave privada del emisor obteniéndose la firma digital, luego esta firma junto al mensaje que va a ser cifrado son enviados a través de la red SWIFT.

En el lado del receptor, la firma digital es descifrada con la clave pública del emisor obteniéndose el código hash, y en paralelo al mensaje ya descifrado se ejecuta la función hash, luego se comparan ambos códigos hash y al ser iguales, el receptor puede estar seguro de la autenticidad del emisor y de la integridad de la información.

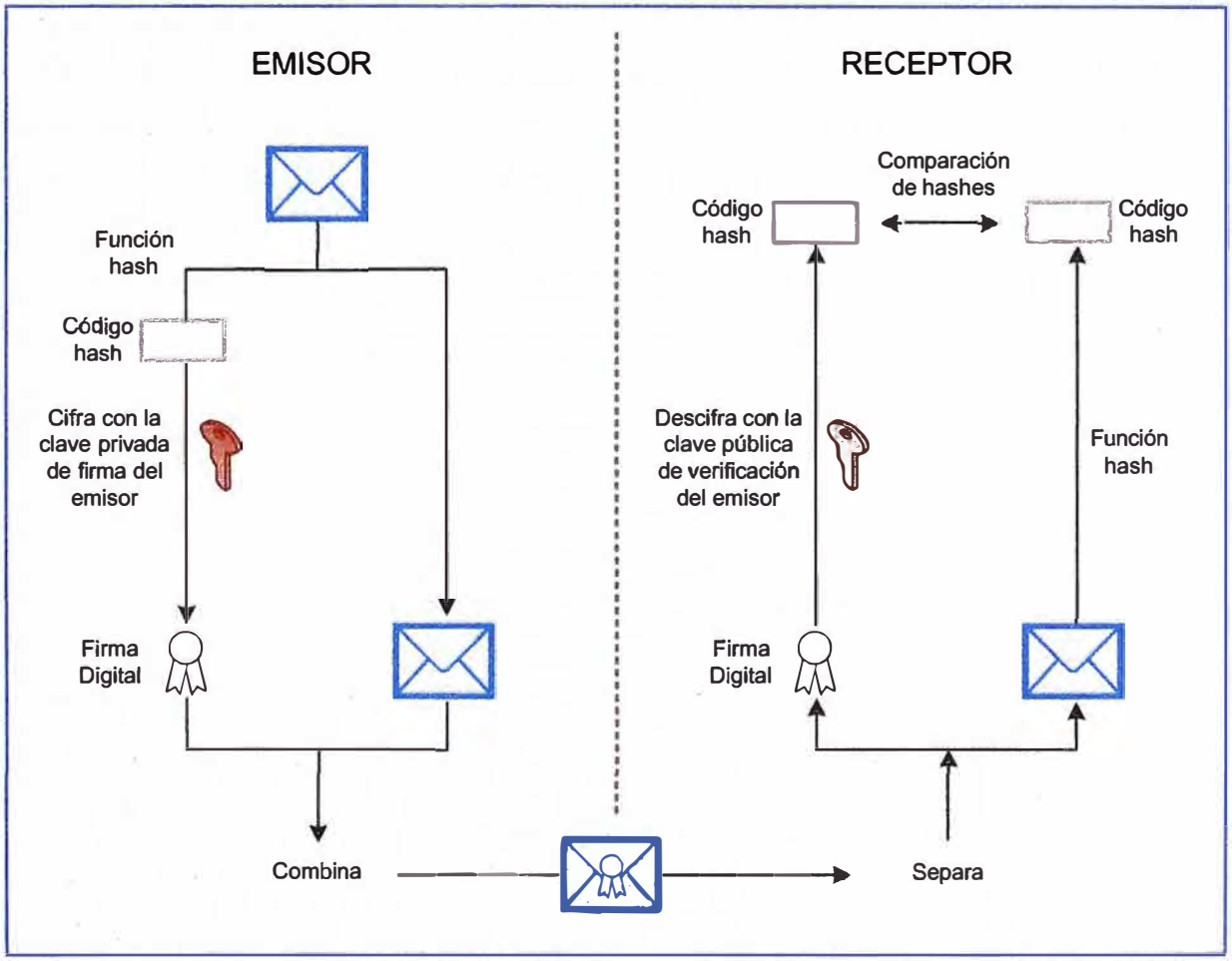

Figura 3.14 - Firma digital y verificación de la firma de un mensaje financiero

En la infraestructura de claves públicas de la red SWIFT, la firma digital de un mensaje financiero emplea lo siguiente:

- Algoritmo RSA (2048 bits) para la pareja de claves de firma asimétrica
- Función hash (algoritmo SHA-256)

3.3.1 Función Hash

Una función hash es una función que se aplica al mensaje, dando como resultado un valor resumido llamado código hash.

Una propiedad fundamental de la función hash es que si a dos mensajes se aplica una misma función hash y se obtienen dos códigos hash diferentes, quiere decir que los dos mensajes de entrada que generaron esos dos resultados también son diferentes [9].

Las funciones de hash son algoritmos que se emplean en muchas aplicaciones, por ello son utilizadas con los algoritmos de clave pública para el cifrado y la firma digital. Una función hash es también utilizada en la verificación de la integridad, y en la autenticación (no repudio de origen) del mensaje recibido.

La función hash que se aplica al mensaje financiero usa el algoritmo SHA-256 (Secure Hash Algorithm) que es un algoritmo de has seguro que calcula una representación condensada de un mensaje o de un archivo de datos.

Esta representación condensada es de una longitud fija y se conoce como un resumen del mensaje o huella digital. Debido a la conjetura de que es computacionalmente imposible producir dos mensajes que tengan el mismo resumen del mensaje, se puede usar este resumen como parte de la integridad de los datos y como control de comparación.

En la Figura 3.15 se ilustra el uso de la función hash sobre el mensaje para obtener el código hash, luego este código se cifra con la clave privada de firma para obtener la firma digital.

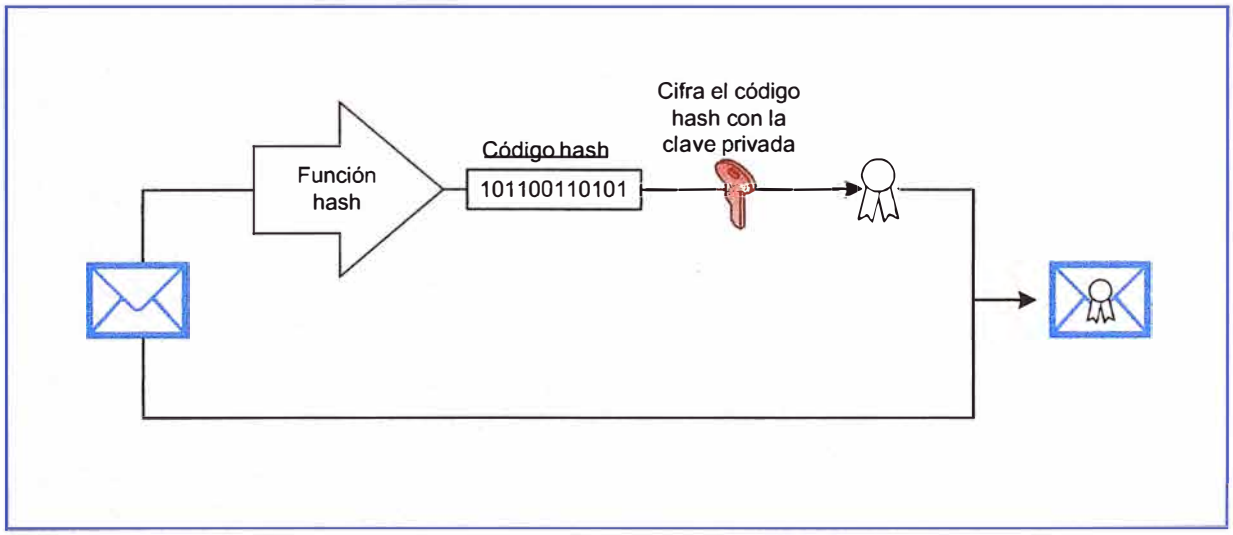

Figura 3.15 - Uso de la función y código hash para obtener la firma digital

En la Figura 3.16 se ilustra el uso de la función hash sobre el mensaje para obtener el código hash, y en forma paralela la firma digital se descifra con la clave pública de verificación del emisor obteniéndose otro código hash, y si ambos códigos hash son iguales quiere decir que la firma digital es válida.

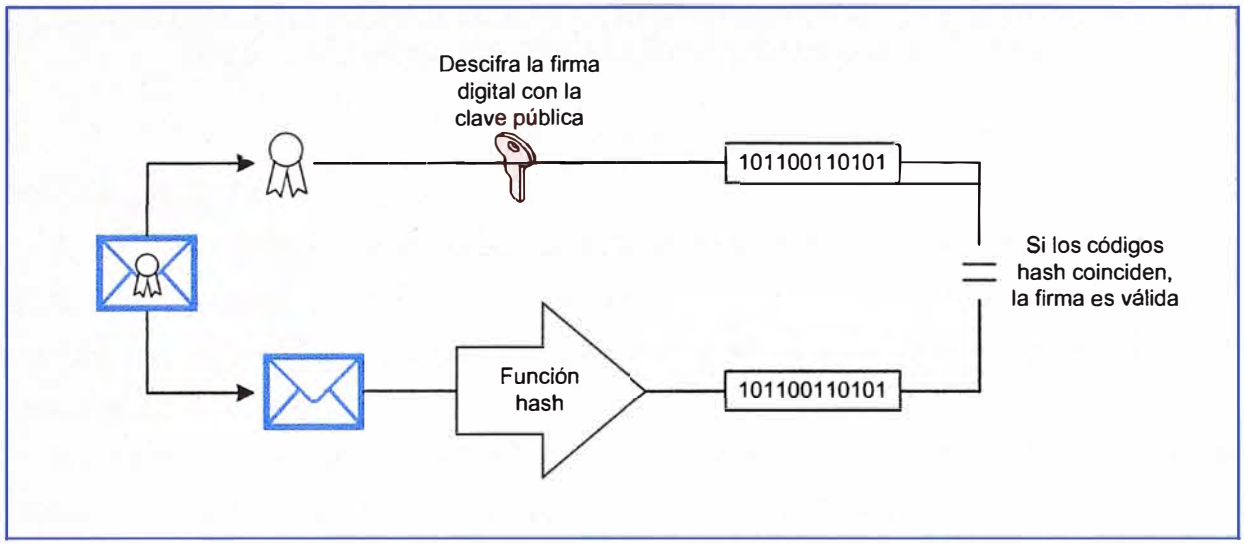

Figura 3.16 - Uso de la función y código hash para la verificación de la firma digital

CAPÍTULO IV
ESTUDIO DE CASO: SEGURIDAD DE TRANSFERENCIA INTERBANCARIA ENTRE DOS INSTITUCIONES FINANCIERAS USANDO SWIFT-HSM

4.1 Introducción

El mensaje financiero es elaborado en el lado de la institución financiera emisora, que es el lugar donde se aplica el cifrado del mensaje por medio de un HSM, una vez que el mensaje se encuentra protegido se procede a enviarlo a la institución financiera receptora.

El mensaje enviado por la institución financiera emisora primero llega a la red SWIFT a través de un network partner, y una vez que el sistema SWIFT valida el mensaje, este mensaje es entregado a la institución financiera receptora a través de otro network partner.

En la institución financiera receptora el mensaje es recibido y descifrado por medio de un HSM.

La Figura 4.1 ilustra como la institución financiera emisora se comunica con la institución financiera receptora a través de los network partners y la red SWIFT.

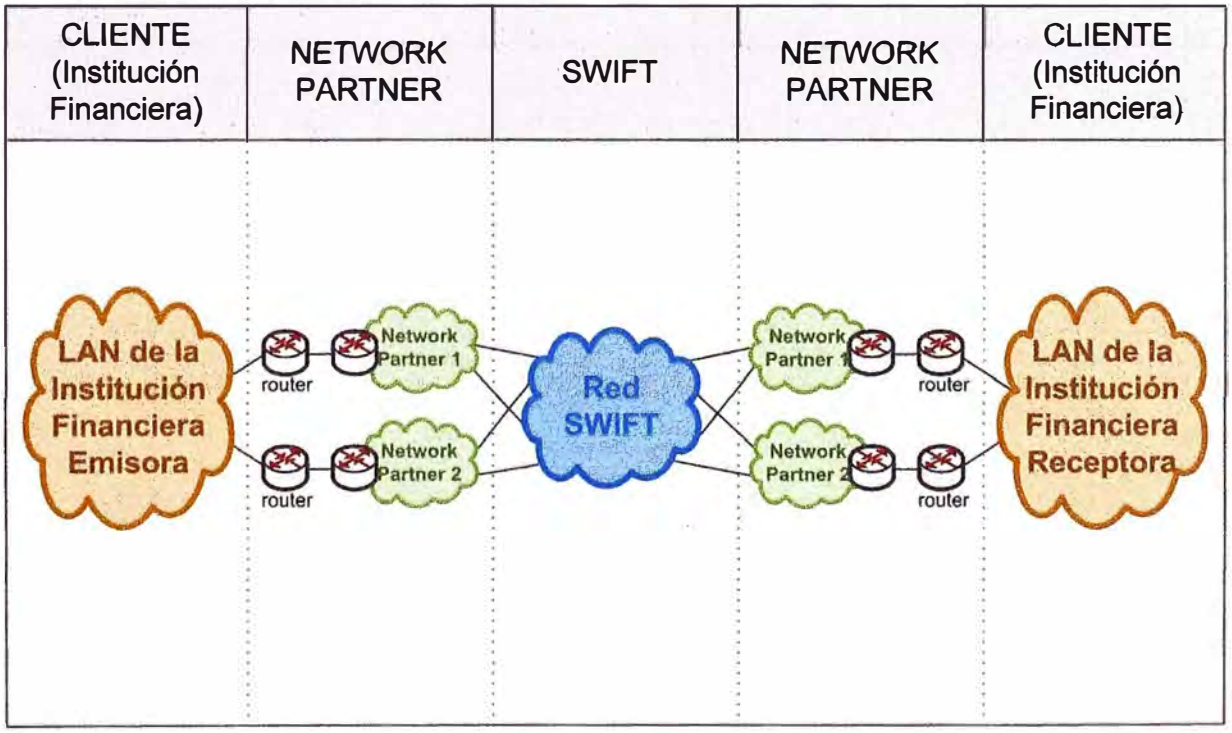

Figura 4.1 - Conectividad entre dos instituciones financieras a través de la red SWIFT y los network partners

4.2 Claves criptográficas en los HSM y en el directorio de la red SWIFT

El HSM de cada institución financiera genera las parejas de claves asimétricas (privada y pública) y la clave simétrica, los cuales son [1][11]:

- Pareja de claves de firma asimétrica (RSA de 2048 bits)
  - Clave privada de firma
  - Clave pública de verificación de firma
- Pareja de claves de encripción asimétrica (RSA de 2048 bits)
  - Clave privada de descifrado
  - Clave pública de cifrado
- Clave de encripción simétrica (triple DES con dos claves de 112 bits), que es una clave secreta y aleatoria

De estas parejas de claves asimétricas, las claves privadas son almacenadas y protegidas en el HSM, y las claves públicas son enviadas al directorio de la red SWIFT donde son almacenadas.

Las claves simétricas son claves de sesión secreta y aleatoria, es decir, por cada transacción de un mensaje financiero se genera una clave simétrica diferente. Estas claves también son almacenadas y protegidas en el HSM.

La Figura 4.2 ilustra los HSM de dos instituciones financieras donde son almacenadas las claves privadas y las claves simétricas. También muestra al directorio de la red SWIFT, el cual almacena las claves públicas de estas dos instituciones financieras [2].

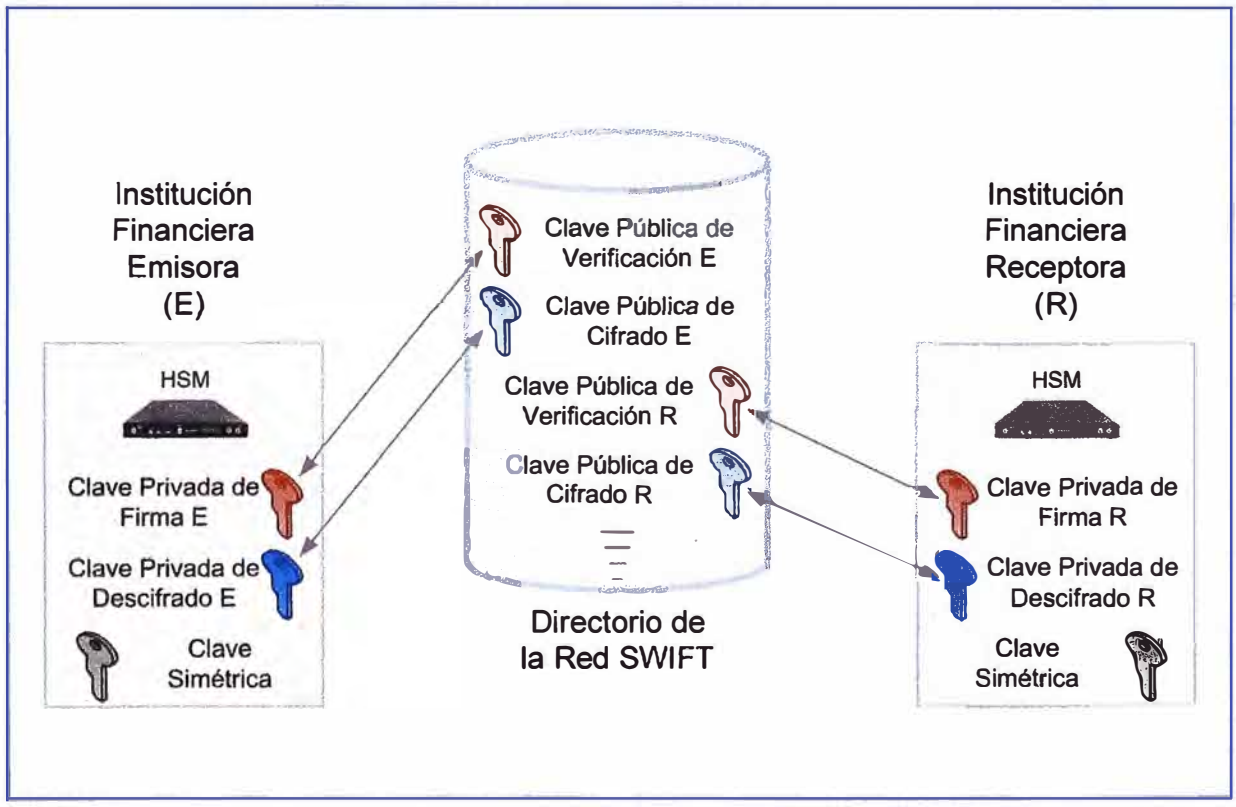

Figura 4.2 - Claves criptográficas en los HSM y en el directorio de la red SWIFT

4.3 Transferencia de pago simple entre dos instituciones financieras

En el presente caso de estudio se muestra una transferencia de pago simple entre dos instituciones financieras, donde se explicará el proceso de encriptamiento, el HSM y su respectiva conectividad.

El presente caso se refiere a una transacción de pago simple que realiza una empresa, el cual en SWIFT se representa por el tipo de mensaje MT103 que viene a ser una transferencia de pago simple que realiza una institución financiera de la empresa ordenante, hacia la institución financiera de la empresa beneficiaria. Esta transacción de pago se representa por un mensaje financiero, el cual al ser enviado de una institución a otra tiene que garantizarse su confidencialidad, autenticidad, integridad y no repudio [13][16].

La Figura 4.3 ilustra el caso de estudio, donde la empresa Robbins Ltd. ordena a su institución financiera Chase Manhattan Bank, Londres (CHASGB2LXXX), a realizar una transferencia de pago simple a la empresa Chocobelge NV a través de su institución financiera Fortis Bank, Bruselas (GEBABEBBXXX).

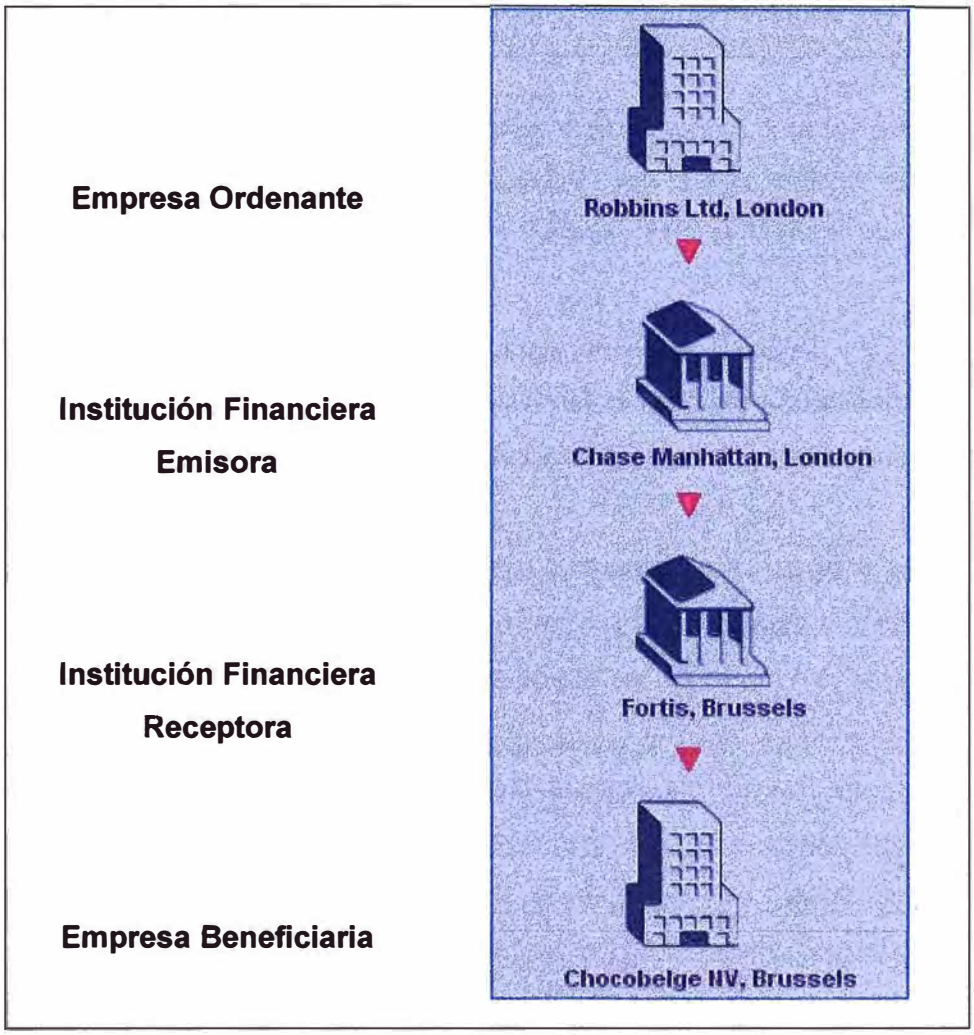

Figura 4.3 - Las cuatro partes involucradas en la transferencia de pago

Las cuatro partes involucradas en un mensaje MT103 (como se ilustra en la Figura 4.3), son las siguientes:

- La empresa ordenante (Robbins Ltd.), que tiene una cuenta en la institución financiera emisora
- La institución financiera emisora (Chase Manhattan Bank), que es la institución de la empresa ordenante
- La institución financiera receptora (Fortis Bank), que es la institución de la empresa beneficiaria
- La empresa beneficiaria (Chocobelge NV), que tiene una cuenta en la institución financiera receptora

4.4 Conectividad de la institución financiera emisora a la red SWIFT

Para el presente caso de estudio en el lado de la institución financiera emisora (Chase Manhattan Bank) se considera lo siguiente [6]:

- La empresa ordenante (Robbins Ltd., Londres) solicita a su institución financiera a realizar una transferencia de pago simple a la empresa beneficiaria (Chocobelge NV, Bruselas).
- La institución financiera emisora (Chase Manhattan Bank, Londres) posee dos cajas HSM en clúster (configuración de alta disponibilidad), los cuales realizan los procesos de firma digital y de cifrado de los mensajes financieros (aplicando las claves y los algoritmos criptográficos).
- La institución financiera emisora (Chase Manhattan Bank, Londres) se conecta a la red SWIFT por medio de la conectividad oro, el cual utiliza dos líneas dedicadas a través de dos network partners, donde un network partner es configurado como canal principal y el otro como canal de reserva.
- Un network partner es de la empresa Orange Business Services y el otro network partner es de la empresa Colt, para ello cada network partner instala y configura su router donde el cliente para que el cliente tenga acceso a la red SWIFT a través de cada una de sus propias redes de comunicaciones.

La Figura 4.4 ilustra a la empresa ordenante (Robbins Ltd.), la LAN de la institución financiera emisora (Chase Manhattan Bank) con sus dos cajas HSM en clúster (configuración de alta disponibilidad), su conectividad a la red SWIFT por medio de la conectividad oro que emplea como canal principal la red de comunicaciones del network partner Orange Business Services y como canal de reserva la red de comunicaciones del network partner Colt.

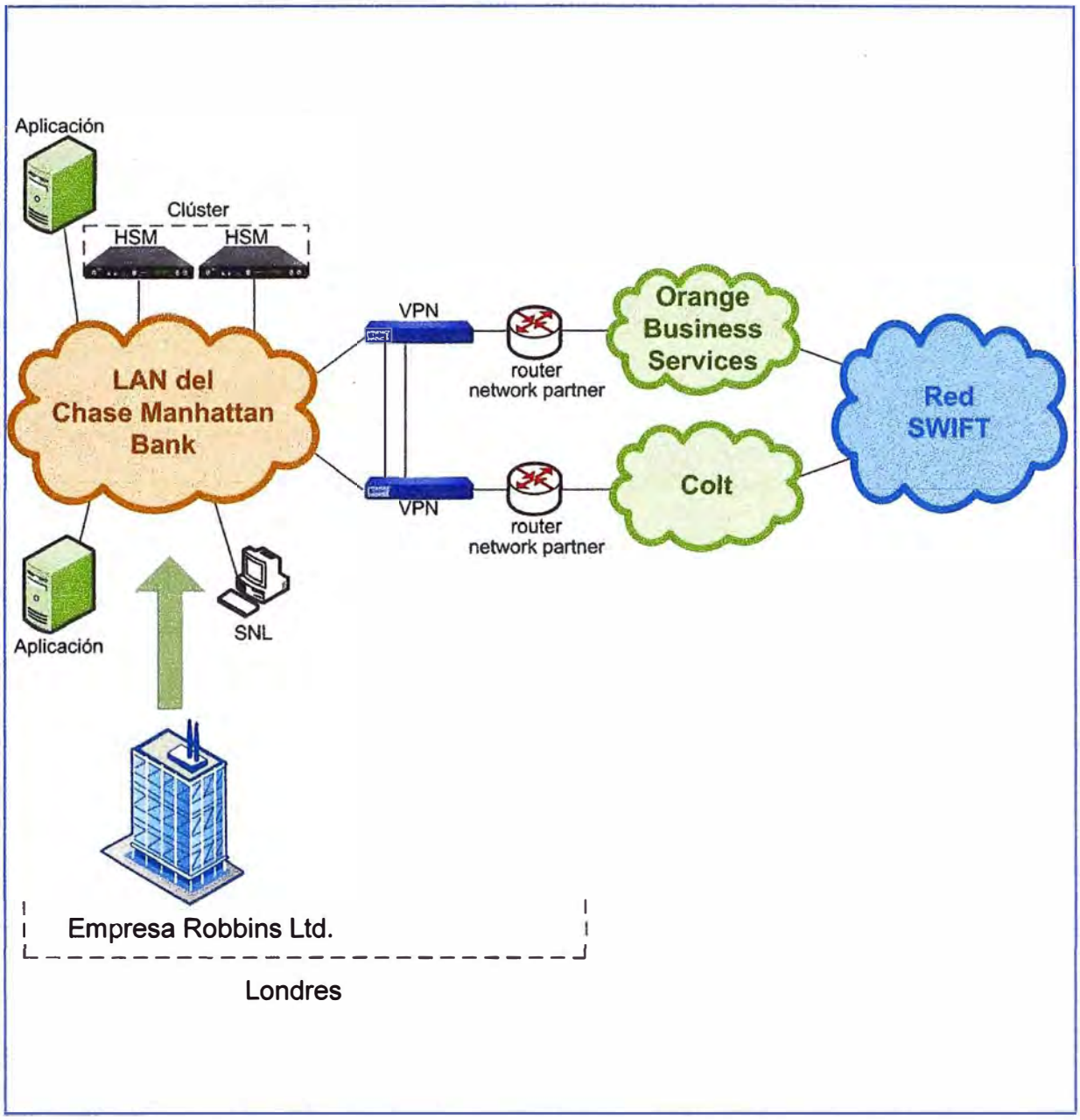

Figura 4.4 - Conectividad de la institución financiera emisora (Chase Manhattan Bank, Londres) a la red SWIFT

4.5 Mensaje financiero en la institución financiera emisora

Una vez recibida la solicitud de la empresa ordenante, la institución financiera emisora procede a elaborar el mensaje financiero que se va a enviar, para ello toma en cuenta los siguientes datos [13]:

- Empresa ordenante:

  Nombre: Robbins Ltd., Londres

  Dirección: 67 Leinster Square Londres SW1X7XOL

  Detalles de pago: Factura N° 33898

- Institución financiera emisora:

Nombre: Chase Manhattan Bank

Código BIC: CHASGB2LXXX

Dirección: Woodlgate Houde Coleman Street Londres EC2P 2HD

Referencia: 494931/DEV

Cantidad: 356000

Moneda: EUR

Fecha valor: 27 abril 2002

- Institución financiera receptora:

Nombre: Fortis Bank NV, Bruselas

Código BIC: GEBABEBBXXX

- Empresa beneficiaria:

Nombre: Chocobelge NV

Dirección: Rue de l'Armistice 5 1020 Bruselas

Número de cuenta: 001-9394230-49

Firma digital y cifrado del mensaje financiero

Antes de ser enviado el mensaje financiero MT103 desde la institución financiera emisora (Chase Manhattan Bank), el HSM interactúa con el mensaje ya elaborado aplicándole las operaciones criptográficas (la firma digital y el cifrado), cuyos pasos se detallan a continuación [11]:

- Al mensaje ya terminado (ingresado todos los datos y en el momento de enviarlo) se le aplica la función hash, creándose un código hash.
- El código hash se cifra asimétricamente con la clave privada de firma del emisor (usando el algoritmo RSA), creándose la firma digital.
- La firma digital se añade al mensaje.
- Luego el mensaje se cifra simétricamente con la clave secreta simétrica (usando el algoritmo triple DES).
- También la clave secreta se cifra asimétricamente con la clave pública de cifrado del receptor (usando el algoritmo RSA).
- Ambos, tanto el mensaje firmado y cifrado, como la clave secreta cifrada, son enviados a través de la red SWIFT al receptor.

La Figura 4.5 ilustra un diagrama de secuencia de pasos que se le aplica al mensaje financiero en su proceso de firma digital y cifrado, usando para ello las claves criptográficas que entregan el HSM y el directorio de la red SWIFT y cuyas operaciones criptográficas (aplicando el algoritmo simétrico triple DES y el algoritmo asimétrico RSA, y la clave privada de firma del emisor y la clave pública del receptor) se realizan en las cajas HSM que se encuentran en clúster.

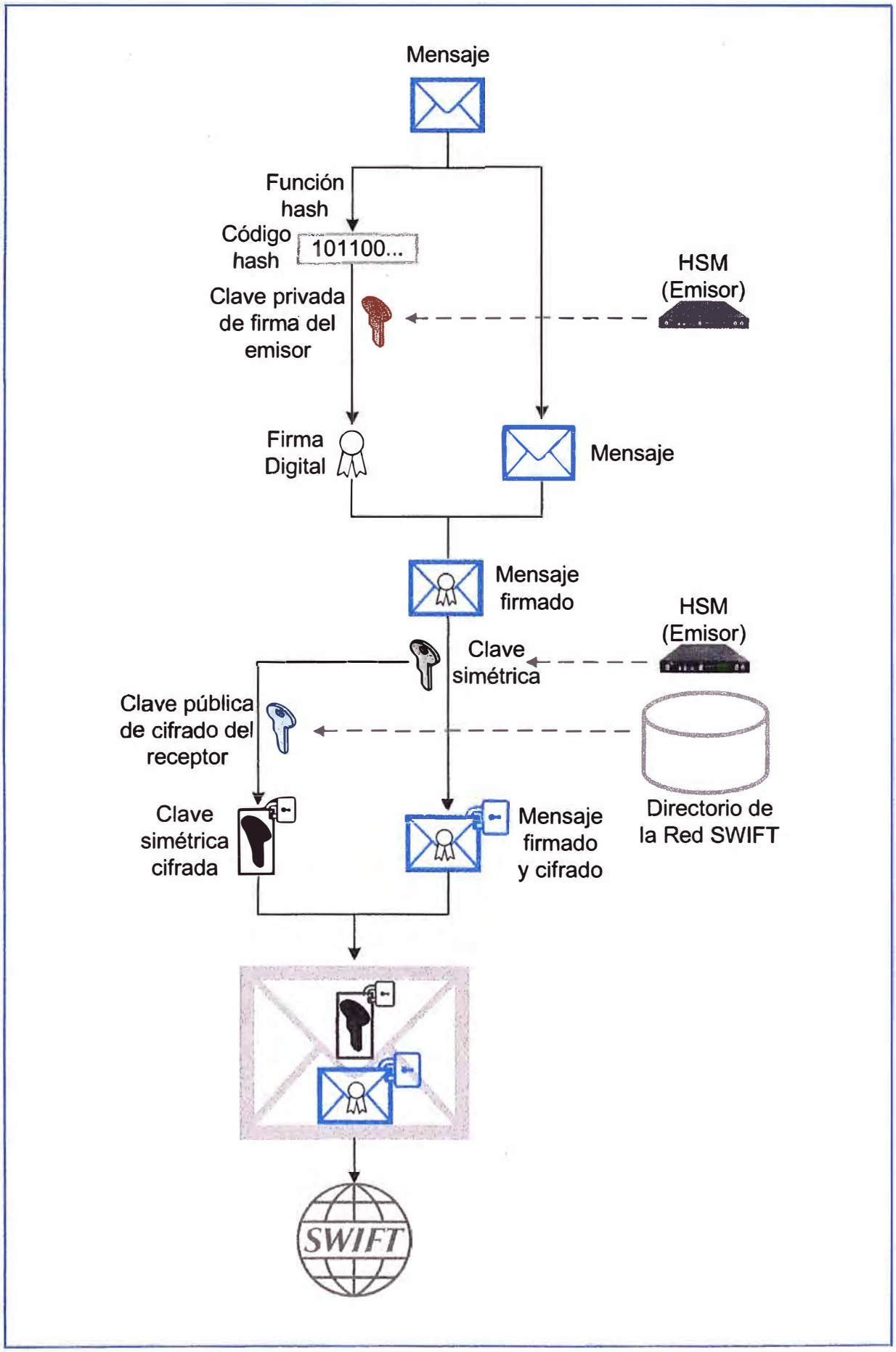

Figura 4.5 - Aplicando la firma y el cifrado al mensaje financiero por medio del HSM

Finalmente, el mensaje MT103 firmado y cifrado en la institución financiera emisora (Chase Manhattan Bank) es enviado a través de la red SWIFT a la institución financiera receptora (Fortis Bank) como se ilustra en la Figura 4.6

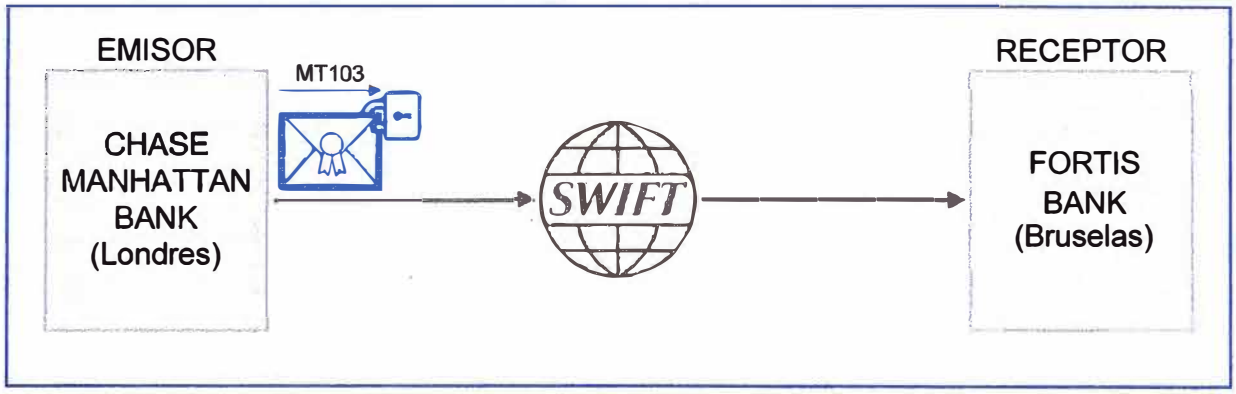

Figura 4.6 - El Chase Manhattan Bank envía un mensaje MT103

4.6 Mensaje financiero en la red SWIFT

Luego que la institución financiera emisora (Chase Manhattan Bank) envió el mensaje MT103, este mensaje es recibido por el sistema SWIFT.

La Figura 4.7 ilustra al sistema SWIFT guardando dos copias del mensaje MT103 y luego envía un ACK al emisor para indicar que su mensaje fue enviado exitosamente.

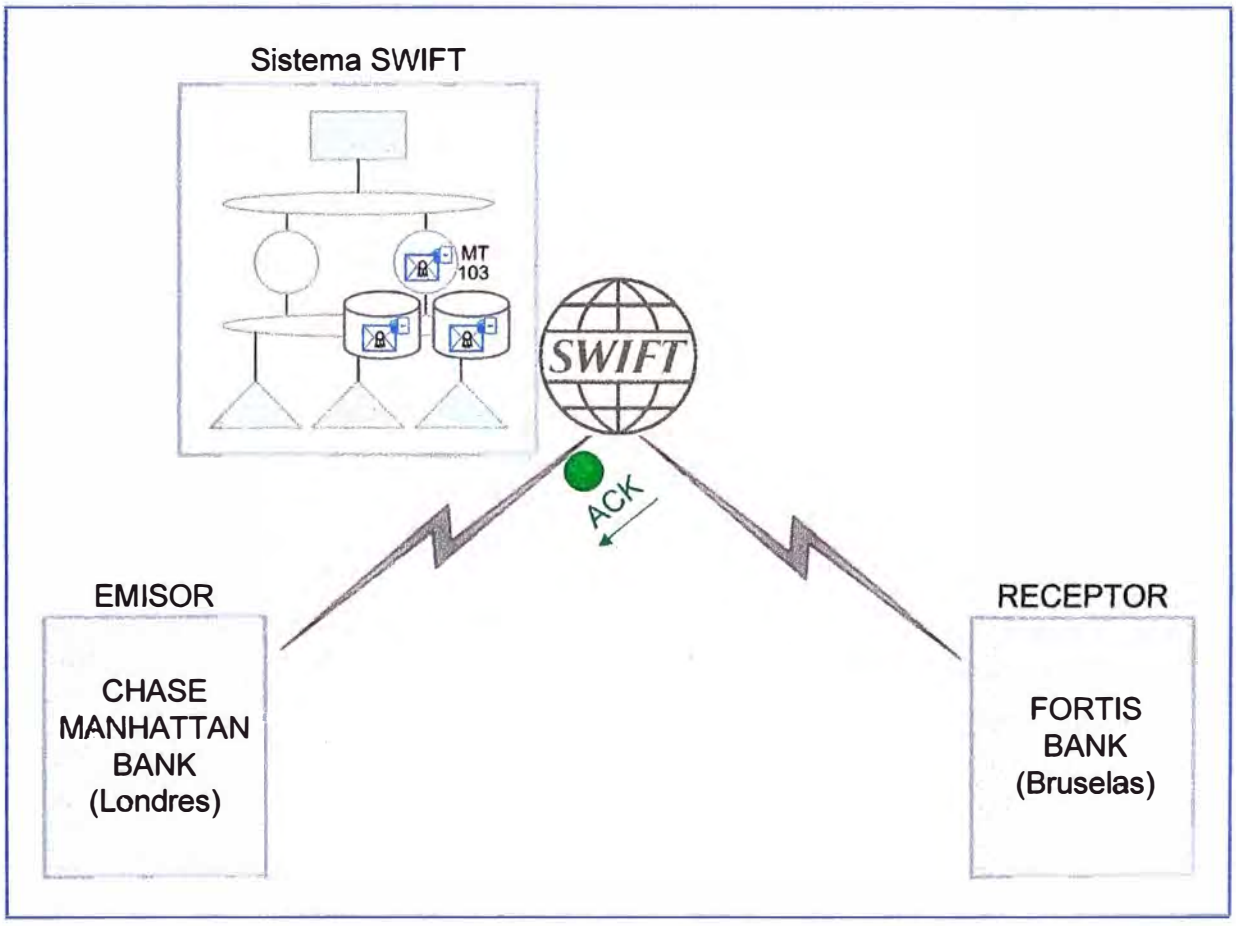

Figura 4.7 - El sistema SWIFT envía un ACK al Chase Manhattan Bank

De la Figura 4.7 se observa que el mensaje es recibido y reconocido positivamente (ACK, Positive Acknowledgement) por el sistema SWIFT, por ello este mensaje es guardado en dos unidades de almacenamiento diferentes por un período de 124 días, luego envía un ACK a la institución financiera emisora como una medida de control indicando que su mensaje fue enviado exitosamente. En el caso que el mensaje es recibido y reconocido negativamente (NAK, Negative Acknowledgement) por el sistema SWIFT, este mensaje también es guardado y luego envía un NAK a la institución financiera emisora como una medida de control indicando que su mensaje no tiene la estructura correcta y tiene que ser enviado de nuevo [16].

Una vez que la institución financiera emisora (Chase Manhattan Bank) recibe el ACK de parte del sistema SWIFT, quiere decir que su mensaje MT103 fue considerado válido. Luego el sistema SWIFT procede a entregar el mensaje MT103 a la institución financiera receptora (Fortis Bank).

La Figura 4.8 ilustra a la institución financiera emisora recibiendo el ACK e inmediatamente después el sistema SWIFT procede a enviar el mensaje MT103 a la institución financiera receptora.

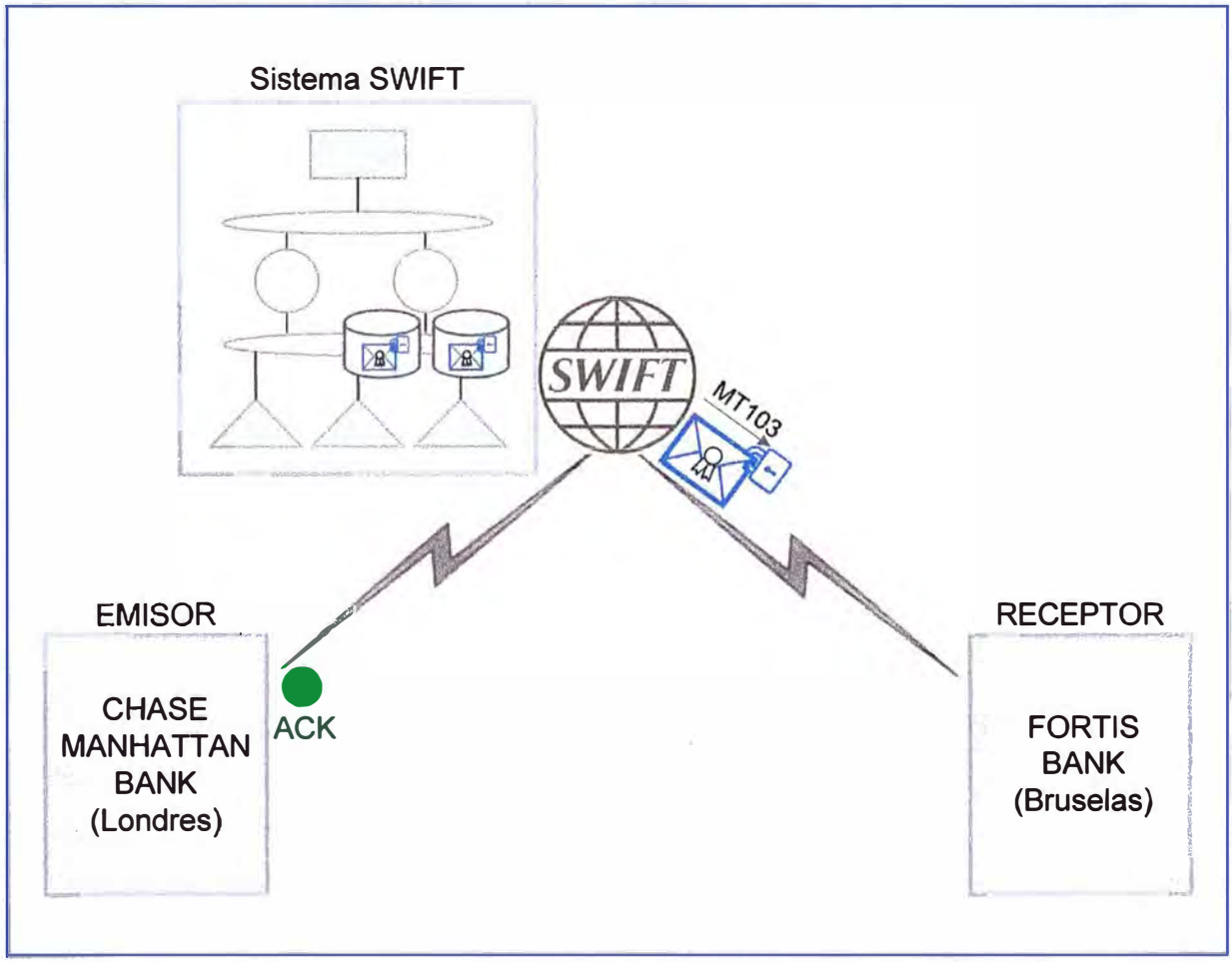

Figura 4.8 - El sistema SWIFT envía el mensaje MT103 a la institución financiera receptora (Fortis Bank)

Una vez que la institución financiera receptora (Fortis Bank) recibe el mensaje MT103, esta institución financiera envía un UAK (Positive User Acknowledgement) al sistema SWIFT para confirmarle que el mensaje MT103 ha sido aceptado. Si la institución financiera receptora envía un UNK (Negative User Acknowledgement) quiere decir que el mensaje MT103 no ha sido aceptado.

La Figura 4.9 ilustra a la institución financiera receptora recibiendo el mensaje MT103 e inmediatamente después envía un UAK al sistema SWIFT para confirmarle que el mensaje MT103 ha sido aceptado.

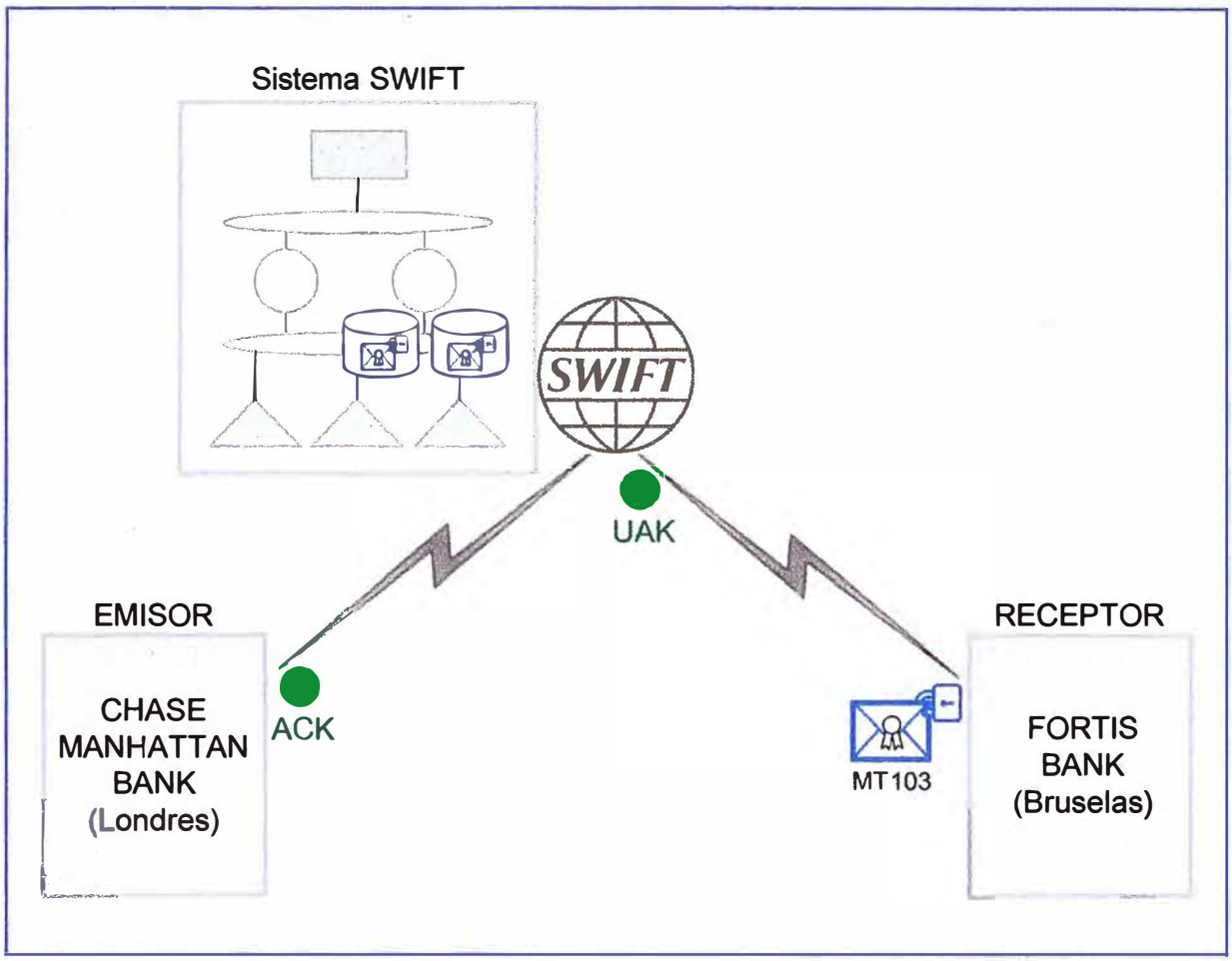

Figura 4.9 - El sistema SWIFT recibe un UAK de la institución financiera receptora (Fortis Bank)

4.7 Conectividad de la institución financiera receptora a la red SWIFT

Para el presente caso de estudio en el lado de la institución financiera receptora se considera lo siguiente [7]:

- La empresa beneficiaria (Chocobelge NV., Bruselas) recibe una transferencia de pago en su número de cuenta de su institución financiera (Fortis Bank, Bruselas).
- La institución financiera receptora (Fortis Bank, Bruselas) posee dos cajas HSM en clúster, los cuales realizan el proceso de encriptamiento de los mensajes financieros.

- La institución financiera receptora (Fortis Bank, Bruselas) se conecta a la red SWIFT por medio de la conectividad oro, el cual utiliza dos líneas dedicadas a través de dos network partners, donde un network partner es configurado como canal principal y el otro como canal de reserva.
- Un network partner es de la empresa AT & T y el otro network partner es de la empresa BT Infonet, para ello cada network partner instala y configura su router donde el cliente para que el cliente tenga acceso a la red SWIFT a través de cada una de sus propias redes de comunicaciones.

La Figura 4.10 ilustra a la empresa beneficiaria (Chocobelge NV.), la LAN de la institución financiera receptora (Fortis Bank) y su conectividad a la red SWIFT por medio de la conectividad oro empleando los network partners AT & T y BT Infonet los cuales utilizan líneas dedicadas.

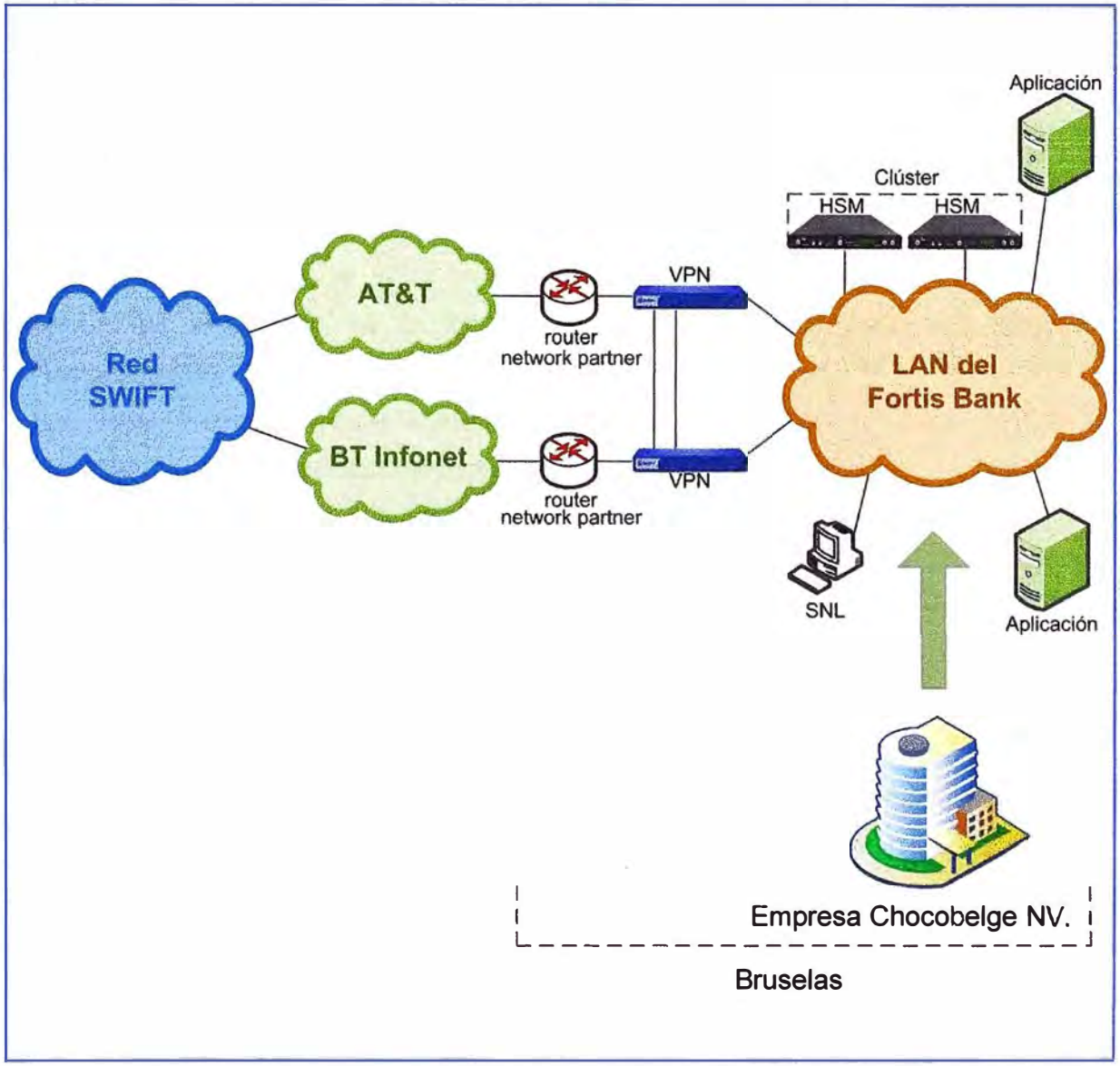

Figura 4.10 - Conectividad de la institución financiera receptora (Fortis Bank, Bruselas) a la red SWIFT

4.8 Mensaje financiero en la institución financiera receptora

La institución financiera receptora (Fortis Bank) recibe el mensaje MT103 de la institución financiera emisora (Chase Manhattan Bank) a través de la red SWIFT, como se ilustra en la Figura 4.11.

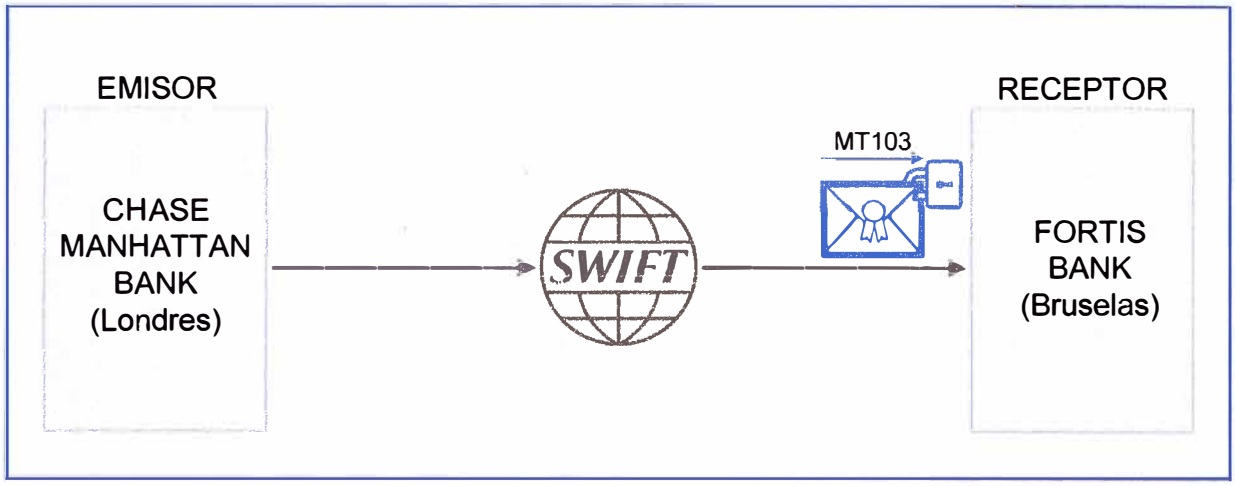

Figura 4.11 - Mensaje MT103 recibido por el Fortis Bank

Verificación de la firma y descifrado del mensaje

Una vez recibido el mensaje financiero MT103 por parte de la institución financiera receptora (Fortis Bank), el HSM interactúa con el mensaje recibido aplicándole los procesos de verificación de la firma y el descifrado, cuyos pasos se detallan a continuación [11]:

- La clave secreta cifrada se descifra asimétricamente con la clave privada de descifrado del receptor (usando el algoritmo RSA).
- El mensaje cifrado se descifra simétricamente con la clave secreta ya descifrada (usando el algoritmo triple DES).
- Para verificar la firma digital, ésta se descifra asimétricamente con la clave pública de verificación de firma del emisor (usando el algoritmo RSA), obteniéndose un código hash.
- En paralelo, también se ejecuta la función hash al mensaje ya descifrado, obteniéndose otro código hash.
- Ambos códigos hash son comparados, y al ser iguales se verifica que es la firma digital.

La Figura 4.12 ilustra un diagrama de secuencia de pasos que se le aplica al mensaje financiero en su proceso de verificación de firma y descifrado, usando para ello las claves que entregan el HSM y el directorio de la red SWIFT cuyas operaciones criptográficas (aplicando el algoritmo simétrico triple DES y el algoritmo asimétrico RSA, la clave pública de verificación de firma del emisor y la clave privada de descifrado del receptor) se realizan en el HSM.

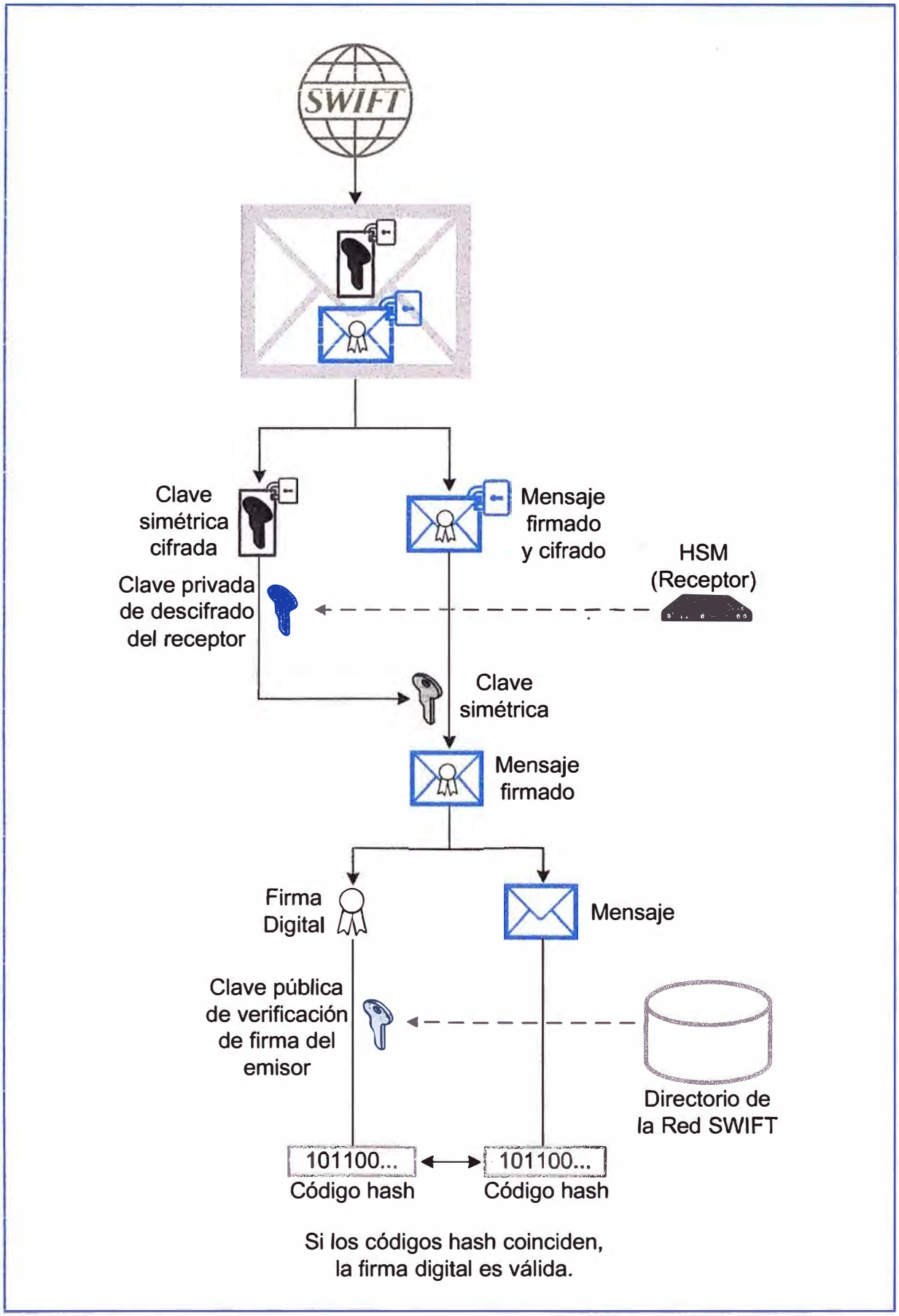

Figura 4.12 - Aplicando la verificación de la firma y el descifrado del mensaje financiero por medio del HSM

CONCLUSIONES Y RECOMENDACIONES

Al término de la elaboración del presente informe se obtiene las siguientes conclusiones y recomendaciones:

1. La seguridad de la información del mensaje financiero no solo se garantiza por las técnicas de encriptamiento, también se garantiza por la red de comunicaciones SWIFT sobre el cual se traslada, debido a que esta red es segura y fiable.
2. SWIFT entrega los HSM a sus clientes para obtener una configuración estandarizada en sus módulos de seguridad de hardware. Si un cliente obtiene un HSM que no es entregado por SWIFT, todas sus operaciones criptográficas sobre los mensajes financieros no serían validados por SWIFT.
3. Las claves criptográficas contenidas en las cajas HSM solo pueden ser copiadas en la otra caja que se encuentra en clúster, es decir, estas claves no pueden ser copiadas fuera del clúster (por ejemplo: un servidor de archivos o de base de datos).
4. El encriptamiento por software es lento porque se instala en un computador que comparte sus recursos informáticos (como memoria, procesador) con otras aplicaciones. El encriptamiento por hardware es rápido porque dedica todos los recursos informáticos del dispositivo de hardware para realizar todas las operaciones criptográficas.
5. Las cajas HSM tienen la particularidad de tener mayor resistencia a la intrusión física, como el manipuleo. Si se detecta una intrusión de desmontaje o modificación del mismo, este dispositivo debe ser capaz de borrar los parámetros de seguridad críticos.
6. SWIFT es sometido a supervisión debido a su importancia de hacer que todo el sistema financiero internacional funcione sin problemas, por ello se forma un comité que periódicamente revisa muchos puntos informáticos, como en el presente caso: la longitud de la clave o el tipo de algoritmo a emplear, para así poder mitigar los riesgos operacionales. Cuando el respectivo comité observe que la longitud de la clave o el algoritmo actual ya no son tan seguros, considerará realizar los cambios apropiados.
7. Un buen sistema de cifrado pone toda la seguridad en la clave y ninguna en el algoritmo, es decir, para un atacante no debería ser de mucha ayuda conocer el algoritmo que se está utilizando. Sólo si el atacante obtuviera la clave, le serviría conocer el

algoritmo. Debido a que toda la seguridad está en la clave, el espacio de claves posibles debe de ser muy amplio.

8. Actualmente, los ordenadores pueden descifrar claves con extrema rapidez, y ésta es la razón por la cual el tamaño de la clave es importante en la criptografía moderna. Por lo tanto, el tamaño de la clave es una medida de la seguridad del sistema. También es importante el período de renovación de la clave, debido a que es más difícil detectarlo cuanto más corto es el período de renovación.

9. El triple DES es un algoritmo simétrico que está desapareciendo lentamente, siendo reemplazado por el algoritmo simétrico AES. Por su diseño, el DES y por lo tanto el triple DES son algoritmos simétricos lentos. Actualmente, el algoritmo AES puede llegar a ser hasta 6 veces más rápido y es un algoritmo simétrico mucho más seguro, por ello es recomendable que se considere este punto en el comité de seguridad informática que supervisa periódicamente a SWIFT.

10. Es recomendable que las cajas HSM tengan una configuración de alta disponibilidad, es decir se encuentren en clúster para evitar tiempos muertos ante la inoperatividad de uno de ellos.

ANEXO A
Definición de términos

VPN (Virtual Private Network)

Es un dispositivo electrónico que cifra todo el tráfico entre la instalación del cliente y el entorno controlado por SWIFT. La función principal de la caja VPN es crear y administrar un túnel seguro entre las instalaciones del cliente y el punto de backbone administrado por SWIFT.

Router

Es un dispositivo de hardware que se emplea para la interconexión de redes informáticas. Este dispositivo permite asegurar el direccionamiento de los paquetes de datos entre las redes para determinar la mejor ruta que se debe tomar.

SNL (SWIFTNet Link)

Es el producto de software obligatorio de SWIFT para los usuarios de la red SWIFT. SNL garantiza el acceso del cliente a la red SWIFT al ofrecer una ventana de acceso única y consistente. Sus funcionalidades incluyen transporte, formateo, seguridad y gestión de servicios.

SSL (Secure Socket Layer)

La capa de conexión segura (SSL) es un protocolo criptográfico que proporciona una comunicación segura en una red. En este caso, el SSL protege la comunicación entre el SNL y cada una de las cajas HSM, y también entre las cajas HSM en un clúster, a través de la encriptación de datos y de la autenticación de dos vías. El canal SSL usa dos canales TLS autenticados y bidireccionales.

TLS (Transport Layer Security)

La seguridad de la capa de transporte (TLS) es un protocolo criptográfico que proporciona una comunicación segura en una red. Las operaciones criptográficas y las operaciones de administración de claves son ejecutadas a través de una conexión SSL/TLS entre el SNL y la caja HSM.

SSH (Secure Shell)

Es un protocolo que permite acceder a equipos remotos a través de una red. En este caso, el enlace administrativo entre el SNL y el HSM es asegurada con una conexión SSH, el cual es un estándar para accesos o inicios de sesión seguros.

RoHS (Restriction of Hazardous Substances)

Es una directiva que restringe el uso de seis materiales peligrosos (plomo, mercurio, cadmio, cromo VI, PBB, PBDE) en la fabricación de varios tipos de equipos electrónicos y de equipos eléctricos. RoHS es conocida como la directiva “libre de plomo”.

FCC (Federal Communications Commission)

La comisión federal de comunicaciones se encarga de elaborar normas de compatibilidad electromagnética en lo que se refiere a equipos electrónicos. Esta norma

permite al equipo tener una limitación en sus posibles emisiones electromagnéticas, para reducir las interferencias electromagnéticas dañinas, principalmente en los sistemas de comunicación.

FCC clase B parte 15

Esta norma indica que las emisiones de radiofrecuencia del equipo son tan bajas que no interfieren con otros dispositivos tales como la radio y la televisión.

Certificado X.509v3

El X509 es un estándar para las infraestructuras de claves públicas, es decir da un formato estándar para los certificados de claves públicas. En X.509, una autoridad certificadora (en este caso, la autoridad de certificación de la red SWIFT) emite un certificado asociando una clave pública con los datos que permiten identificar al titular.

G-10

Es el grupo de los diez bancos centrales que cooperan con el Banco Nacional de Bélgica en la supervisión de SWIFT. Estos diez bancos son: Bank of Canada, Deutsche Bundesbank, Banque de France, Banca d' Italia, Bank of Japan, De Nederlandsche Bank, Sveriges Riksbank, Swiss National Bank, Bank of England y Federal Reserve System (EE.UU.), representado por el Federal Reserve Bank of New York y el Consejo de Gobernadores del Federal Reserve System.

NIST (National Institute of Standards and Technology)

El Instituto Nacional de Normas y Tecnología (NIST) es una agencia que se encarga de promover la innovación y la competitividad industrial en los Estados Unidos. Este instituto tiene como labor establecer los patrones de medida y las normas y estándares de la tecnología.

ANEXO B
Estándares federales de procesamiento de la información (FIPS 140)

Los estándares federales de procesamiento de la información 140 (FIPS, Federal Information Processing Standards) son una norma que coordina los requerimientos de los módulos criptográficos, así como otros aspectos de seguridad informática para el uso de la información confidencial. Esta norma garantiza el uso de métodos y algoritmos de cifrado seguros y fuertes. También se aplica sobre cualquier producto (hardware o software) que se encarga de almacenar o transmitir información confidencial.

FIPS 140 son un conjunto de normas de seguridad, de los cuales:

- La norma FIPS 140-1 se publicó el 11 de enero de 1994, pero fue reemplazada por la norma FIPS 140-2.
- La norma FIPS 140-2 se publicó el 25 de mayo de 2001, la cual es la norma actual.

La norma FIPS 140-3 es una nueva versión que se encuentra actualmente en fase de desarrollo y es probable que en poco tiempo sustituya a la norma FIPS 140-2.

La norma FIPS 140-2 define cuatro niveles de seguridad, el cual especifica el nivel de seguridad al que se ajusta el producto.

- El nivel 1, es el más bajo, que normalmente se usa en productos de cifrado de software e impone requisitos de seguridad muy limitados.
- El nivel 2 requiere la capacidad para detectar la intrusión física mediante sistemas de bloqueo físico.
- El nivel 3 añade mayor resistencia a la intrusión física con fines de modificación o de desmontaje, de forma que dificulta con intensidad los ataques. También incluye protección criptográfica y administración de claves, y de una separación física o lógica entre las interfaces mediante el cual se accede a los parámetros de seguridad crítica.
- El nivel 4 está diseñado para productos que operan en entornos desprotegidos físicamente, por ello requiere una protección física más estricta que haga frente a los ataques del medio ambiente.

ANEXO C
Mensaje financiero MT103 estructurado

La Figura C-1 ilustra como el mensaje financiero MT103 queda estructurado al ser ingresados todos los datos mencionados en el caso de estudio, los cuales representan una transacción de pago simple. En este caso, este mensaje representa una notificación (ACK) de SWIFT hacia la institución financiera emisora de que su mensaje MT103 fue enviado exitosamente.

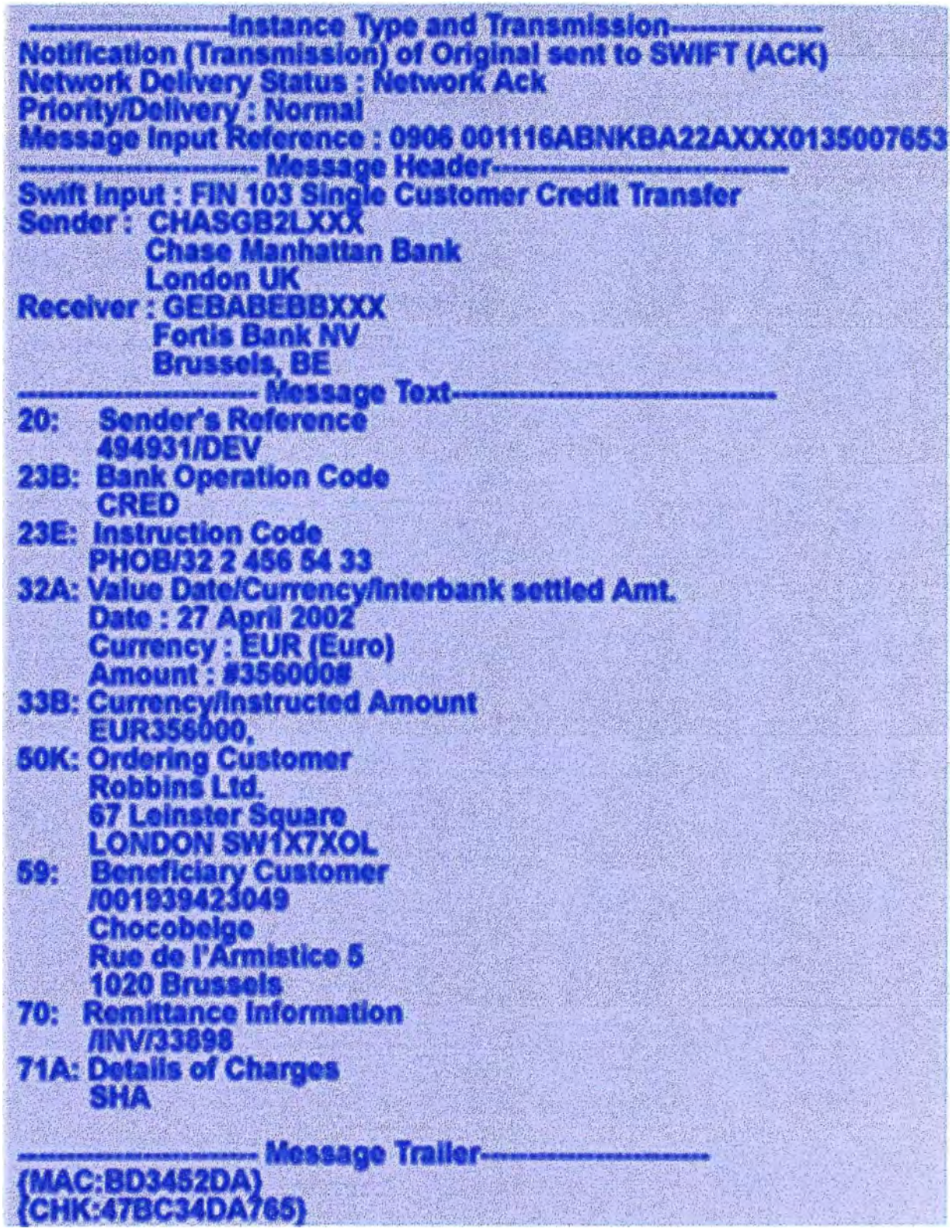

Figura C-1 - Mensaje financiero MT103 estructurado

Como se observa de la Figura C-1 la cabecera del mensaje contiene:

- Tipo de mensaje: 103
- Emisor: Chase Manhattan Bank
- Receptor: Fortis Bank

Y como se observa de la Figura C-1 el texto del mensaje contiene los siguientes campos (en base a los datos mencionados del caso de estudio):

- Campo 20: Referencia del emisor: 494931/DEV
- Campo 32A: Fecha valor / Moneda / Cantidad

  Fecha: 27 abril 2002

  Moneda: EUR

  Cantidad: 356000
- Campo 50K: Empresa ordenante Robbins Ltd.
- Campo 59: Empresa beneficiaria Chocobelge

  Número de cuenta: 001939423049
- Campo 70: Información del emisor

  Factura N° 33898

BIBLIOGRAFIA

[1] SWIFT, "Certificate Administration Guide of SWIFTNet PKI", guía de SWIFT, Bélgica, 2007

[2] SWIFT, "Installation and Administration Guide of SWIFTNet Link", guía de SWIFT, Bélgica, 2007

[3] SWIFT, "Network Access Control Guide of SWIFTNet", guía de SWIFT, Bélgica, 2006

[4] SWIFT, "HSM Equipment – Quick Start Guides", guías de SWIFT, Bélgica, 2006

[5] SWIFT, "Service Description of Alliance Connect Bronze", documento de SWIFT, Bélgica, 2009

[6] SWIFT, "Service Description of Alliance Connect Silver", documento de SWIFT, Bélgica, 2009

[7] SWIFT, "Service Description of Alliance Connect Gold", documento de SWIFT, Bélgica, 2009

[8] SWIFT, "Service Description of SWIFTNet", documento de SWIFT, Bélgica, 2007

[9] Manuel José Lucena López, "Criptografía y Seguridad en Computadores", 2001

[10] Víctor Bravo y Antonio Araujo, "Criptografía", documento de CENDITEL, 2008

[11] BCG (Business Computer Group), "Public Key Infrastructure en SWIFTNet", manual de BCG (curso de capacitación), Perú, 2006

[12] BCG (Business Computer Group), "Seminario sobre SWIFTNet", manual de BCG (curso de capacitación), Perú, 2006

[13] BCG (Business Computer Group), "Managing SWIFTAlliance Access", manual de BCG (curso de capacitación), Perú, 2005

[14] SWIFT, "About SWIFT", http://www.swift.com/about_swift/index.page?, página SWIFT, última fecha de acceso: 02/09/2011

[15] SWIFT, "BIC", http://www.swift.com/products/bic_registration, página SWIFT, última fecha de acceso: 02/09/2011

[16] SWIFT, "Documentation (User Handbook)", documentación SWIFT, 2011