(19) OFICINA ESPAÑOLA DE PATENTES Y MARCAS

ESPAÑA

(11) Número de publicación: **2 294 843**

(51) Int. Cl.:
H04K 1/00 (2006.01)
H04M 1/68 (2006.01)
H04M 3/42 (2006.01)
H04L 9/00 (2006.01)

(12) TRADUCCIÓN DE PATENTE EUROPEA T3

(86) Número de solicitud europea: **99923846 .2**
(86) Fecha de presentación : **02.06.1999**
(87) Número de publicación de la solicitud: **1084542**
(87) Fecha de publicación de la solicitud: **21.03.2001**

(54) Título: **Sistema y procedimiento para el acceso protegido a la red.**

(30) Prioridad: **02.06.1998 US 89156**

(45) Fecha de publicación de la mención BOPI:
01.04.2008

(45) Fecha de la publicación del folleto de la patente:
01.04.2008

(73) Titular/es: **Snapshield Ltd.**
Habarzel Street 2, Ramat Hachayal
Tel Aviv, 69710, IL

(72) Inventor/es: **Naor, Uri;**
Zigdon, Shimon y
Gonen, Zion

(74) Agente: **Isern Jara, Jorge**

DESCRIPCIÓN

Sistema y procedimiento para el acceso protegido a la red.

Campo de la invención

La presente invención se refiere a sistemas de comunicación y, más específicamente, a un sistema y a un procedimiento para proporcionar comunicaciones protegidas en la red de teléfonos.

Antecedentes de la invención

La red de teléfonos (comúnmente referida como la red pública de teléfonos conmutados o "PSTN" - Public Switched Telephone Network) consiste en una amplia red de instalaciones de conmutación de teléfonos interconectados. Típicamente un equipo telefónico tal como por ejemplo un teléfono, una máquina de fax, o un módem se conecta a la PSTN a través de la instalación telefónica referida como la oficina central o de intercambio local ("CO" - Central Office). Cada CO, a su vez, se conecta a una o más instalaciones de conmutación en la PSTN. A través de esta disposición, el equipo telefónico puede realizar una llamada que es encaminada a través de la CO, a través de la red, a través de otra CO y, finalmente, a otro equipo telefónico.

La parte de la red entre el equipo de intercambio local y el equipo de las instalaciones del cliente (por ejemplo, el equipo telefónico instalado, por ejemplo, en la residencia o en el lugar de trabajo de los clientes) es conocida como la red de acceso (por ejemplo, un bucle local). La red de acceso típicamente consiste en cables de cobre, cables de fibra óptica, cables coaxiales o una combinación de estos o bien otros componentes. Estos componentes pueden transportar señales analógicas o digitales, cualquiera de las cuales puede ser utilizada en diferentes partes de la misma red de acceso. Cuando una red de acceso incluye ambas partes analógicas y digitales, la parte digital de la red de acceso puede terminar en una caja de conexiones colocada fuera de las instalaciones de los clientes. Pares de cables de cobre corren desde la caja de conexiones, a través de las instalaciones de los clientes (por ejemplo, el edificio en donde el cliente tiene el teléfono), hasta el equipo de las instalaciones de los clientes ("CPE" - Customer Premises Equipment).

En general, puede resulta relativamente difícil realizar escuchas ilegales de determinadas comunicaciones de los clientes fuera de la red de acceso. Las líneas de unión de la PSTN que conectan la CO a otro equipo de conmutación típicamente pueden transportar señales digitales multiplexadas. Aquí, una única línea de unión (por ejemplo, un cable de cobre o un cable de fibra óptica) pasa simultáneamente las señales para un gran número de llamadas. Por lo tanto, es muy difícil que una persona que realice una escucha ilegal determine cuál de las líneas de unión en la CO y en la PSTN están transmitiendo las comunicaciones de un cliente específico. Además, puede ser relativamente difícil que una persona que realice una escucha ilegal extraiga estas señales en el caso en el que la persona que realice la escucha ilegal tenga éxito en la identificación de la línea de unión de los clientes.

Por el contrario, la red de acceso es más susceptible a las escuchas ilegales. Proporcionada la ruta de la red de acceso a través de espacios públicos, las personas que realizan escuchas ilegales pueden tener un acceso relativamente fácil a la red de acceso de los clientes en algún punto a lo largo de su ruta hasta la CO. Por lo tanto, puede ser relativamente fácil identificar una red de acceso de un cliente específico y derivar el cable. En particular, la parte de la red de acceso que funciona por cables de cobre fuera de las instalaciones de los clientes es especialmente susceptible a las escuchas ilegales.

Algunos sistemas convencionales utilizan dispositivos de encriptación en un intento de proporcionar comunicaciones protegidas por las redes telefónicas. Típicamente, un dispositivo de encriptación/desencriptación está conectado al equipo telefónico en cada extremo de la llamada. Por ejemplo, las señales desde un teléfono en un extremo de la llamada son encaminadas a otro de estos dispositivos, encriptadas, y enviadas entonces a la PSTN. Las señales encriptadas son encaminadas a través de la PSTN y eventualmente a otro dispositivo. Ese dispositivo desencripta las señales y proporciona las señales desencriptadas al teléfono en el otro extremo de la llamada.

Sistemas tales como el que se acaba de describir tienen diversas desventajas. Por ejemplo, ambos clientes deben tener el equipo de encriptación/desencriptación. Esto requiere que las partes preparen el sistema con anterioridad. De modo que, estos sistemas no son muy eficaces desde el punto de vista de los costes para las partes a excepción de que realicen un número relativamente grande de llamadas entre sí. Además, en algunos de estos sistemas, las personas que llaman deben establecer manualmente la conexión de seguridad después de llamar a la otra parte. Esto puede resultar incómodo y puede facilitar que las personas que realizan escuchas ilegales determinen el número de teléfono de la parte que ha sido llamada o la parte que llama con relativa facilidad. Además, en muchos de estos sistemas, las llamadas a destinos que no tienen equipo de encriptación/desencriptación son inseguras. En vista de estas y otras desventajas, existe la necesidad de un procedimiento más eficaz para proporcionar comunicaciones protegidas en la red telefónica.

El documento EP-A-0 642 277 expone una red de telecomunicaciones provista de un nodo de seguridad accesible desde cualquier ubicación conectada a la red y que funciona para transformar información desde un formato encriptado a uno no encriptado. El documento US-A-4,815,128 expone aparatos de pasarelas los cuales buscan proporcionar una comunicación protegida entre abonados autorizados previamente determinados que operan en una red de radio y una red telefónica y determina si señales de mensajes transparentes o codificados se van a encaminar de una red a la otra

sin la utilización de una desencriptación y encriptación de intervención para conseguir la interconexión. El documento US-A-5,222,136 expone un sistema para el intercambio de datos encriptados utilizando claves de intercambio de claves públicas y privada.

Resumen de la invención

Un sistema construido de acuerdo con la invención proporciona comunicaciones protegidas entre equipos de instalaciones de clientes y un nodo de conmutación en la red tal como un intercambio local. Las comunicaciones desde el equipo de un abonado son encriptadas antes de ser enviadas a la red de acceso. Estas comunicaciones son desencriptadas por el equipo instalado en el nodo de la red. Las comunicaciones al abonado son encriptadas en el nodo de la red y desencriptadas entonces en el lado del abonado de la red.

En una forma de realización en la que sólo una de las partes que participa en una llamada es un abonado, las comunicaciones están protegidas sólo entre el CPE del abonado y el equipo en el nodo de la red. Por ejemplo, una unidad de encriptación/desencriptación está instalada entre el CPE del abonado y el lado del abonado de la red de acceso. Otra unidad de encriptación/desencriptación está instalada en la CO que proporciona el servicio telefónico al abonado. En este caso, el sistema no encripta las comunicaciones del abonado en el resto de la red. Como resultado, el abonado se puede comunicar con equipo remoto que no esté protegido disponiendo todavía de comunicaciones protegidas en la red de acceso del abonado.

En una forma de realización en las que más de una de las partes que participan en la llamada es un abonado, las comunicaciones se pueden proteger entre cada uno de los CPE de los abonados. En este caso, una unidad de encriptación/desencriptación está instalada entre cada uno de los CPE de los abonados y aquel lado del abonado de la red de acceso. Además, una unidad de encriptación/desencriptación está instalada en algún nodo de la red (por ejemplo, en una CO). Las comunicaciones desde cada abonado son encaminadas a través de la unidad de encriptación/desencriptación en el nodo de la red. De esta manera, el sistema proporciona comunicaciones protegidas terminal a terminal entre cada uno de los abonados.

En una forma de realización, el equipo de encriptación/desencriptación instalado en la red es un centro de múltiples líneas de encriptación/desencriptación que está conectado a un conmutador en la red telefónica a través de interfaces digitales (por ejemplo, E1, T1, ISDN). Las llamadas a través de la red que necesitan ser desencriptadas o encriptadas son encaminadas a través del centro de encriptación/desencriptación y entonces de vuelta a la red. Esta forma de realización utiliza una tecnología de integración de telefonía e informática ("CTI" - Computer Telephony Integration) para proporcionar un sistema que sea relativamente fácil de adaptar al usuario y de ampliar.

En resumen, el sistema protege las comunicaciones sobre la parte más susceptible de la red: la red de acceso del abonado. Además, el sistema protege las comunicaciones en la red de acceso del abonado incluso cuando uno de los participantes en la llamada no tenga equipo de encriptación/desencriptación.

De forma significante, el sistema protege la llamada antes de que cualquier información importante sea enviada por la red de acceso. Esto se consigue estableciendo una conexión protegida en la red de acceso del abonado anises de establecer la conexión telefónica con la parte a la que se llama. Como resultado, el sistema puede encriptar el número de teléfono de destino marcado por la parte que llama antes de que envíe este número por la red de acceso. Además, el sistema puede encriptar información de identificación automática del número que el sistema recibe de una parte que llama al abonado. Esto es, el número de teléfono de la parte que llama puede ser encriptado antes de ser enviado a la red de acceso.

Un sistema construido de acuerdo con la invención puede ser más eficaz desde el punto de vista de los costes que los sistemas convencionales porque el sistema puede ser configurado de forma que un banco relativamente pequeño de unidades de encriptación/desencriptación sobre la base de la red maneje llamadas de un número relativamente grande de abonados. En este caso, la relación de unidades de encriptación/desencriptación con respecto a los abonados se puede basar en un análisis estadístico de la utilización del tráfico de llamadas protegidas.

Breve descripción de los dibujos

Estas y otras características de la invención se harán más evidentes a partir de la siguiente descripción y de las reivindicaciones, cuando se consideran con los dibujos adjuntos, en los cuales caracteres de referencias iguales se refieren a elementos iguales a través de los mismos y en los cuales:

la figura 1 es un diagrama de bloques de una red telefónica que incorpora una forma de realización de un sistema de encriptación/desencriptación de red construido de acuerdo con la invención;

la figura 2 es un diagrama de un procedimiento de establecimiento de una llamada para una llanada protegida de salida (por ejemplo, una llamada originada a partir de un abonado protegido) de acuerdo con una forma de realización de la invención;

la figura 3 es un diagrama de un procedimiento de establecimiento de una llamada para una llamada protegida de entrada (por ejemplo, una llamada realizada a un abonado protegido) de acuerdo con una forma de realización de la invención;

la figura 4 es un diagrama de bloques de una forma de realización de una unidad de encriptación/desencriptación de la instalación de los clientes construida de acuerdo con la invención;

la figura 5 es un diagrama de bloques de una forma de realización de un sistema de conmutación de encriptación/desencriptación basado en la red construido de acuerdo con la invención;

las figuras 6A y 6B son un cuadro de flujo de operaciones de establecimiento de llamada para una llamada originada a partir de un abonado protegido, que pueden ser llevadas a cabo por el sistema de conmutación de encriptación/desencriptación basado en la red de la figura 5;

las figuras 7A y 7B son un cuadro de flujo de operaciones de establecimiento de llamada para una llamada realizada a un abonado protegido, que pueden ser llevadas a cabo por el sistema de conmutación de encriptación/desencriptación basado en la red de la figura 5;

la figura 8 es un diagrama de bloques que ilustra diversas formas de realización de los sistemas de encriptación/desencriptación de la red construidos de acuerdo con la invención; y

la figura 9 es un diagrama de bloques de una red telefónica que incorpora una forma de realización de un sistema de encriptación/desencriptación de la red basada en una red digital de servicios integrados ISDN que está construido de acuerdo con la invención.

Descripción de las formas de realización ejemplares

La figura 1 ilustra un sistema de comunicación S e incluye diversos teléfonos 22 y 24 que se comunican a través de una red pública de telefonía conmutada 20. Cada teléfono 22 y 24 se conecta a una CO 26 y 28 en la red 20 por una red de acceso correspondiente 30 y 32.

De acuerdo con una forma de realización de la invención, una unidad de encriptación/desencriptación 34 instalada en las instalaciones de los clientes 40 coopera con un centro protegido 36 instalado en la red 20 para proporcionar conexiones protegidas en la red de acceso 30. Una llamada hacia y desde el teléfono 22 se establece a través de la unidad de encriptación/desencriptación 34 y el centro protegido 36. Una vez se ha establecido la llamada, señales de salida (es decir, señales desde el teléfono 22 al teléfono 24) son encaminadas a través de la unidad de encriptación/desencriptación 34 a través de la línea 38. La unidad de encriptación/desencriptación 34 encripta estas señales y las envía al centro protegido 36 a través de la red de acceso 30 y el equipo de conmutación en la CO 26. El equipo de conmutación de la CO envía las señales por la línea 44 a un puerto de entrada del centro protegido 36. Típicamente, el centro protegido 36 está colocado en el mismo edificio que el equipo de conmutación de la CO.

El centro protegido 36 desencripta las señales encriptadas y las envía por la red de acceso existente al teléfono 24. Las señales son encaminadas desde el puerto de salida del centro protegido 36, por la línea 46 y al equipo de conmutación de la CO. La CO 26 encamina la señal desencriptada a otra CO 28 en la red 20. Como se representa mediante la línea discontinua 42, la llamada se puede establecer a través de otro equipo de conmutación (no representado) en la red 20. Después de que la señal desencriptada llegue a la CO 28, la CO 28 envía la señal al teléfono 24 por la red de acceso 32.

Las señales de entrada (es decir, las señales enviadas desde el teléfono 24 al teléfono 22) son encaminadas inicialmente a través del centro protegido 36 a través de la CO 26. El centro protegido 36 encripta estas señales, las envía entonces por la red de acceso 30 a la unidad de encriptación/desencriptación 34. La unidad de encriptación/desencriptación 34 desencripta las señales y envía las señales desencriptadas al teléfono 22.

Tanto para las llamadas de entrada como las de salida, el sistema establece dos conexiones telefónicas para cada llamada, una conexión entre el teléfono 22 y el centro protegido 36 y la otra conexión entre el centro protegido 36 y el teléfono 24. En general, los abonados no notarán diferencia alguna entre las llamadas protegidas provistas por el sistema y las llamadas realizadas sin el sistema protegido.

Los procedimientos de establecimiento de llamada para una llamada de salida y una llamada de entrada se describen en las figuras 2 y 3, respectivamente. Las entidades del sistema S están representadas por líneas verticales tal como se indica. Las dos fronteras de la PSTN 20 (lado 30 de la red de acceso y lado 32 de la red de acceso) están representadas como PSTN 20A y PSTN 20B, respectivamente. Los procedimientos de llamada están representados a modo de líneas verticales de tiempo con las operaciones subsiguientes representadas en niveles sucesivamente inferiores del diagrama.

La figura 2 es un diagrama de un procedimiento de establecimiento de llamada para una llamada originada desde un abonado protegido (por ejemplo, el teléfono 22). El procedimiento arranca cuando se coge el receptor del teléfono 22 (es decir, el teléfono 22 se descuelga). Esto está representado por la línea 50 en la parte superior izquierda del

diagrama. La unidad de encriptación/desencriptación 34 detecta la condición de descolgado en la línea 38 (figura 1) y envía un tono de marcado (representado por la línea 52) al teléfono 22 por la línea 38.

También en respuesta a la condición de descolgado, la unidad de encriptación/desencriptación 34 realiza una llamada a un centro protegido 36 a través de la red de acceso 30 (línea 54). La unidad de encriptación/desencriptación 34 mantiene una lista de números de teléfono de centros protegidos 36 en el área local de la unidad. Esta lista se puede ordenar de acuerdo con la proximidad del centro protegido 36 a la unidad de encriptación/desencriptación 34 o de acuerdo con otros factores tales como los respectivos cargos por uso adicional. Cuando la unidad de encriptación/desencriptación 34 recibe una señal de ocupado de la red o cuando el centro protegido 36 no contesta la llamada, la unidad de encriptación/desencriptación 36 puede llamar a otro número de teléfono de la lista. Como se describe más adelante en este documento, los números en la lista pueden haber sido programados dentro del dispositivo por el abonado o actualizados automáticamente por el centro protegido 36.

Un conmutador en la PSTN 20A (por ejemplo, CO 26) procesa la llamada y envía una señal de timbre al centro protegido 36 a través del puerto de entrada 44 (línea 56). En respuesta, el centro protegido contesta la llamada (por ejemplo, "coge" la línea) y envía una señal de iniciación a la unidad de encriptación/desencriptación 34 (línea 58). Si la unidad de encriptación/desencriptación 34 responde con la señal de reconocimiento apropiada, la unidad de encriptación/desencriptación 34 y el centro protegido 36 se comunican para establecer una conexión de módem entre ellos.

Después de que se haya establecido la conexión entre la unidad de encriptación/desencriptación 34 y el centro protegido 36, el centro protegido 36 verifica que la llamada de entrada es de un abonado autorizado (línea 60). Esto se puede conseguir utilizando, por ejemplo, una autentificación Deffie-Helman. El procedimiento de autentificación también puede utilizar un número de identificación personal (PIN - Personal Identification Number) cuando se desea una protección adicional.

A continuación, la unidad de encriptación/desencriptación 34 y el centro protegido 36 intercambian claves de encriptación (línea 62). El centro protegido 36 y la unidad de encriptación/desencriptación 34 soportan algoritmos de claves públicas y privadas. Inicialmente, el centro protegido genera una clave de encriptación y solicita a la unidad de encriptación/desencriptación su clave pública. El centro protegido encripta el número de sesión con la clave pública provista por la unidad de encriptación/desencriptación 34 y envía el número de la sesión encriptado a la unidad de encriptación/desencriptación 34.

El proceso de intercambio de claves se puede conseguir utilizando un procedimiento simétrico. En este caso, la unidad de encriptación/desencriptación 34 genera también una clave aleatoria de sesión que encripta con la clave pública provista por el centro protegido 36. La unidad 34 transmite entonces la clave de la sesión encriptada al centro protegido 36.

Después de que la unidad 34 y el centro protegido 36 tengan la clave simétrica para la sesión, inhabilitan el algoritmo de clave pública y utilizan un algoritmo de clave simétrica para el resto de la sesión. A partir de este punto en adelante, la unidad de encriptación/desencriptación 34 y el centro protegido 36 encripta todas las comunicaciones que pasan entre ellos por el canal de módem protegido. De forma significante, las operaciones expuestas anteriormente se llevan a cabo sin ninguna interferencia con las llamadas.

Como se representa mediante la línea 64 en la figura 2, después de que el abonado reciba el tono de marcado, el abonado marca el número de teléfono del destino deseado (el teléfono 24 en este ejemplo). Un descodificador de multifrecuencia de doble tono (DTMF - Dual Tone Multifrecuency) en la unidad de encriptación/desencriptación 34 captura el número y lo almacena temporalmente. De acuerdo con la invención, la unidad de encriptación/desencriptación 34 no envía esta información al centro protegido 36 hasta que la red de acceso 30 esté protegida (línea 66).

El centro protegido 36 inicia una llamada al teléfono 24 utilizando el número suministrado por la unidad de encriptación/desencriptación 34 (línea 60). Esto es, el centro protegido 36 descuelga un puerto de salida y marca el número de teléfono asignado al teléfono 24. La PSTN 20B realiza la llamada al teléfono 24 (línea 70) y envía las señales apropiadas de progreso de la llamada (por ejemplo, el timbre) al centro de protección 36 (línea 72). El centro de protección, a su vez, pasa estas señales de vuelta al teléfono 22 (línea 74).

Cuando el receptor en el teléfono 24 es "cogido" (línea 76), se establece una conexión entre el teléfono 24 y el centro protegido 36. En respuesta, el centro protegido 36 completa su conexión al teléfono 22 (línea 78). Entonces un mecanismo de encaminamiento interno en el centro protegido 36 (descrito más adelante en este documento) conecta estas dos conexiones para proporcionar la conexión entre los teléfonos 22 y 24.

Como ha sido descrito antes en este documento, todas las comunicaciones entre la unidad de encriptación/desencriptación 34 y el centro protegido 36 están encriptadas. De ese modo, un abonado puede tener una comunicación protegida por su red de acceso mientras esté en comunicación con un equipo inseguro.

La figura 3 es un diagrama de un procedimiento de establecimiento de llamada para una llamada realizada desde un teléfono inseguro (por ejemplo, el teléfono 24) a un teléfono protegido (por ejemplo, el teléfono 22). El proceso arranca cuando el llamador coge el teléfono 24 (línea 80) y llama al teléfono del abonado 22 (línea 82). El número de

teléfono (Y) en la figura 3 es el número protegido asignado a un abonado. Este número puede ser el número protegido, un número de teléfono nuevo, o un prefijo seguido por un número de teléfono normal.

De acuerdo con una forma de realización de la invención, cuando un llamador marca el número de teléfono asignado al abonado, la llamada es encaminada al centro protegido 36 en lugar de a la línea telefónica que está conectada al equipo telefónico del abonado. De este modo, la PSTN 20B encamina la llamada al centro protegido 36 para establecer una conexión entre el teléfono 24 y el centro protegido 36 (línea 84). Después de que el centro protegido 36 conteste la llamada, requiere detalles a la red relativos a la llamada (por ejemplo, el número virtual marcado). El centro protegido 36 registra el número del abonado (Y) y lo relaciona en correspondencia con el número real de un abonado (X) (bloque 86).

En respuesta a la llamada desde el centro protegido 36 al teléfono del abonado 22 (línea 87), la FSTN 20A envía la señal del timbre al teléfono 22 (línea 88). Aquí la unidad de encriptación/desencriptación 34 pasa la señal del timbre a través del teléfono 22 e informa de vuelta sobre el progreso de la llamada a la PSTN 20A. La PSTN 20A, a su vez, envía las señales de progreso de la llamada al centro protegido 36 (línea 89) el cual retransmite el progreso de la llamada al teléfono 24 (línea 90).

Cuando la unidad de encriptación/desencriptación 34 detecta que se ha descolgado el teléfono 22, retransmite esta señal (coger) a la PSTN 20A (línea 91). En este punto, se establece una conexión entre el centro protegido 36 y la unidad de encriptación/desencriptación 34.

De una manera similar a la que ha. sido descrita anteriormente en este documento, el centro protegido 36 verifica que el destino es un abonado autorizado (línea 92) y la unidad de encriptación/desencriptación 34 y el centro protegido 36 intercambian claves de encriptación (línea 93). Desde este punto en adelante, la unidad de encriptación/desencriptación 34 y el centro protegido 36 encriptan todas las comunicaciones que pasan entre ellos.

Entonces el centro protegido 36 conecta la conexión establecida entre el teléfono 22 y el centro protegido 36 (línea 94) y la conexión establecida entre el teléfono 24 y el centro protegido 36 (línea 95). De este modo, se establece la conexión entre los teléfonos 22 y 24. De acuerdo con una forma de realización de la invención, a partir de la figura 3 se puede ver que el centro protegido 36 no envía información crítica (por ejemplo, señales a partir de la conversación telefónica) al teléfono 22 hasta después de que la red de acceso 30 esté protegida.

Otra vez, todas las comunicaciones entre la unidad de encriptación/desencriptación 34 y el centro protegido 36 son encriptadas después de que se establezca la conexión. De este modo, un abonado puede tener comunicaciones protegidas por su red de acceso incluso durante comunicaciones que hayan sido iniciadas por un equipo inseguro.

Con la descripción de alto nivel anterior presente, los detalles relativos a la implantación y el funcionamiento de la unidad de encriptación/desencriptación 34 y del centro protegido 36 se tratarán ahora con mayor detalle.

La figura 4 es un diagrama de bloques de una forma de realización de una unidad de encriptación/desencriptación 34. Una interfaz de línea 100, forma interfaz con una línea 102 (por ejemplo, una red de acceso) que se conecta en algún punto a la PSTN. La interfaz 100 proporciona la terminación apropiada de las señales en la línea, detecta el estado de colgado y transfiere la identificación del llamador ID (a través de la interfaz de identificación del llamador 103), si es aplicable.

La interfaz 100 se conecta a una unidad de convertidor de analógico a digital (“A/D”) y de convertidor de digital a analógico (“D/A”) 104. Esto permite que un procesador de señal digital (“DSP” - Digital Signal Processor) 106 procese las señales que entran en el interior del dispositivo de la PSTN 20 y generar señales para ser enviadas a la PSTN 20.

Por razones similares, el DSP 106 se conecta a otra unidad de convertidor de analógico a digital (“A/D”) y de convertidor de digital a analógico (“D/A”) 108 que, a su vez, se conecta a una interfaz de línea 110. La interfaz de línea 100 se conecta al equipo de las instalaciones de los clientes abonados a través de la línea 112. La interfaz de línea 110 lleva a cabo operaciones tales como la detección del timbre y el estado de colgado y proporciona la terminación apropiada de la línea 112. La línea 112 se puede conectar directamente a un punto terminal (por ejemplo, un teléfono, una máquina de fax, un módem) o se puede conectar a un centro de intercambio privado (“PBX” - Private Branch Exchange) o a otro equipo que, a su vez, se conecta al punto terminal.

El DSP 106 está programado para llevar a cabo el proceso de la llamada y las operaciones de encriptación/desencriptación para la unidad 34. Esto es, el código de software es descargado de una memoria de datos (por ejemplo, memoria flash 113) dentro del DSP 106. El DEP 106 ejecuta el código para llevar a cabo las operaciones correspondientes.

Inicialmente, el DSP 106 está configurado para manejar las operaciones preliminares de establecimiento de llamada. Por ejemplo, el DSP 106 puede interpretar y generar la señalización de comunicación (por ejemplo, utilizando una función de generador/detector DTMF 111) que pasa por las líneas 102 y 112. Cuando la unidad 34 recibe una llamada de entrada, el DSP 106 determina si la llamada es una llamada de voz o una llamada de fax. Esto se puede determinar, por ejemplo, mediante el análisis de los mensajes iniciales de establecimiento de llamada. Cuando la llamada es una

llamada de voz, la unidad 34 descarga el código de codificador/descodificador de voz 115 dentro del DSP 106. Cuando la llamada es una llamada de fax, la unidad 34 descarga el código de codificador/descodificador de fax 117 dentro del DSP 106.

La unidad 34 también descarga el código para otras funciones del DSP desde la memoria flash 113 a la memoria del DSP 106. Por ejemplo, la unidad 34 descarga el código de una norma de encriptación de datos (DES - Data Encryption Standard) 119 para una función de encriptación/desencriptación, una función de módem 121, una función de autentificación Deffie-Helman 123, una función de cancelación del eco 109, así como la función DTMF 111 expuesta anteriormente en ese documento. La memoria del DSP puede ser interior al DSP 106 (como se representa mediante los recuadros en el DSP 106 de la figura 4) o el DSP 106 puede utilizar una memoria externa para su código ejecutable.

Sigue a continuación una breve descripción de algunas de las funciones del DSP 106. Para establecer un canal protegido, la función Deffie-Helman del DSP 123 genera y procesa información de autentificación. La función del módem 121 modula la información de autentificación generada y la envía al convertidor D/A 104. El convertidor D/A 104 convierte la corriente digital modulada a una corriente analógica y la envía al centro protegido 36 a través de la línea 102. Cuando la unidad 34 recibe la información de autentificación de entrada, la función módem 121 demodula la información recibida (después del proceso de conversión A/D) y envía los datos demodulados a la función Deffie-Helman 123.

Para las llamadas de voz, la información de voz recibida a través de la línea 112 es digitalizada mediante el convertido A/D 108 y encaminada a la función de codificador de la voz 115. La función de codificador de la voz 115 comprime la corriente de datos de entrada (típicamente 64 kbit/s) en una corriente de datos de 8 kbit/s. La función DES 119 encripta esta corriente y la envía a la función de módem 121. Entonces, al igual que antes, la corriente digital modulada es convertida a analógica y enviada al centro protegido 36.

La información de voz recibida a través de la línea 102 es digitalizada por el convertidor A/D 104 y encaminada a la función de módem 121. La función de módem 121 demodula la señal y la envía a la función DES 119. La función DES 119 desencripta esta corriente y la envía a la función de descodificador de la voz 115. La función de descodificador de la voz 115, a su vez, descomprime la corriente de datos de 8 kbit/s en, por ejemplo, una corriente de datos de 64 kbit/s. El convertidor D/A 108 convierte esta corriente digital a analógica y la envía al punto terminal apropiado a través de la línea 112.

Para las llamadas de fax, la información de fax recibida a través de la línea 112 es digitalizada por el convertidor A/D 108 y encaminada a la función de codificador de fax 117. La función de codificador de fax 117 codifica la corriente de datos de entrada (típicamente 14,4 kbit/s, 9,6 kbit/s, etc.) en una corriente de datos de 8 kbit/s. Esta corriente es procesada entonces como ha sido descrito antes en este documento.

De forma similar, la información de fax recibida a través de la línea 102 es demodulada y desencriptada. La información desencriptada es encaminada entonces a una función de descodificador de fax 117 que descodifica los datos como sea necesario. Estos datos son convertidos entonces a analógicos y enviados por la línea 112.

Las operaciones descritas antes en este documento pueden ser implantadas en una variedad de modos diferentes. Por ejemplo, en una forma de realización el DSP 106 soporta operaciones de autentificación de clave pública de módem V.32, de codificador de voz G.729A, FAXRELAY, encriptación/desencriptación DES de 56 bit y Deffie-Helman de 512 bit. Una persona experta en la técnica apreciará, sin embargo, que diversas otras técnicas de módem, codificador de voz, codificador/descodificador de fax, encriptación/desencriptación y autentificación pueden ser utilizadas tales como módem V.34, codificador de voz G.723.1, DES de 128 bit (DES triple) y Deffie-Helman de 1024 bit.

La unidad de encriptación/desencriptación 34 incluye también un circuito de derivación 114. El circuito 114 permite que un abonado derive las funciones de protección llevadas a cabo por la unidad de encriptación/desencriptación 34. Puede resultar deseable derivar las funciones de protección en el caso de un fallo de energía o bien por otras razones.

Una pantalla 116, un teclado 118 y un micrófono 120 permiten que el abonado configure el dispositivo, reciba información del progreso de la llamada y lleve a cabo otras operaciones. Por ejemplo, bajo el control de un circuito de control 122, la pantalla puede proporcionar información con respecto al estado de la llamada (marcado) o el nivel de protección (protegido/desprotegido). De forma similar, el altavoz del micrófono puede proporcionar indicaciones audibles (por ejemplo, dos pitidos significan protegido) relativas a diversa información.

El circuito de control 122 proporciona también funciones de programación 124 para configurar la unidad de encriptación/desencriptación 34. Por ejemplo, la unidad 34 puede ser programada por el abonado utilizando el teclado 118 y la pantalla 116. De forma alternativa, la unidad 34 puede ser programada por la CPE (por ejemplo, utilizando el teclado de un teléfono). Típicamente, sin embargo, el dispositivo es programado por el centro protegido 36 durante el proceso de autentificación descrito antes en este documento. En este caso, el circuito de control 122 se comunica con el DSP 106 para enviar y recibir información de programación por la línea 102. Las operaciones de programación pueden incluir el almacenaje de los números de teléfono 126 de centros protegidos locales (descritos más adelante en este documento) o bien otros parámetros 129 en una memoria de datos 128. Además, se pueden programar diversos parámetros de encriptación/desencriptación (por ejemplo, claves 130) dentro de la unidad de encriptación/desencriptación 34.

Como se describe con mayor detalle más adelante, la unidad 34 también puede ser actualizada o reconfigurada remotamente a través de características de descarga remota de software. Brevemente, el software es descargado dentro de la unidad 34 a través de una línea de entrada y almacenado en la memoria flash 113. Es software está disponible entonces para ser descargado de la memoria flash a la memoria del DSP durante el proceso de establecimiento de llamada de la manera expuesta anteriormente en este documento.

Los componentes de la unidad de encriptación/desencriptación 34 se pueden implementar utilizando una variedad de dispositivos. Por ejemplo, en una forma de realización, se puede utilizar un MITEL MH88422-2 para la interfaz de línea 100. Las unidades A/D y D/A 104 y 108 pueden ser AD1847JP CODECS comercializadas por ANALOG DEVICES. El DSP puede ser un TMS320542PGE-2-50 de TEXAS INSTRUMENTS y la interfaz de línea 110 puede ser una tarjeta de interfaz de línea de abonado PBL 3766 comercializada por ERICSSON. La pantalla 116 puede ser una DV16230B comercializada por DATAVISION. Finalmente, el circuito de derivación 114 puede consistir en un conjunto de relés, que funcionan bajo el control del circuito de control 122. Para proporcionar la derivación, los relés están configurados para desconectar las trayectorias de señal entre la línea 102 y la interfaz 100 y entre la línea 112 y la interfaz 110 y proporcionar trayectorias de señal entre las líneas 102 y 112. De nuevo, una persona experta en la técnica apreciará que se pueden utilizar una gran variedad de componentes diferentes en la puesta en práctica de la invención. Además, se apreciará que los componentes y los procesos anteriores pueden ser implantados y miniaturizados en una pastilla integrada o conjunto de pastillas.

Con referencia ahora a la figura 5, se representa un diagrama de bloques de una forma de realización de un centro protegido 36. El centro protegido 36 incluye una o más tarjetas de red 140 (izquierda superior), una o más tarjetas de DSP 142 (derecha) y una tarjeta de interfaz de herramienta de gestión 144 (inferior izquierda). Estos componentes se comunican entre sí a través de un bus multiplexado 146. Para reducir la complejidad de la figura 5, los detalles de los componentes están descritos para uno sólo de cada uno de los componentes.

La tarjeta de red 140 comunica con un nodo de conmutación en la PSTN 20 tal como una CO 26 (figura 1). En la forma de realización de la figura 5, la tarjeta de red 140 incluye una interfaz de línea 150 (una interfaz T1, una interfaz E1 o una interfaz ISDN PRI) para terminar un enlace común T1, E1 o ISDN PRI (línea 151) desde el nodo de conmutación. El enlace común 151 transporta señales de llamada digitales multiplexadas. Por ejemplo, un enlace común El proporciona 30 canales digitales, cada uno de los cuales transporta señales para una llamada. Una persona experta en la técnica apreciará que el centro protegido 36 puede formar interfaz con la PSTN 20 utilizando procedimientos diferentes de aquellos expuestos en la figura 5.

La tarjeta de red 140 incluye un control de encaminamiento de canal 152 y una interfaz de bus 154 para encaminar el tráfico de llamadas desde y hacia las tarjetas DSP 142. Bajo el control del control de encaminamiento de canal 172, las señales para cada canal son encaminadas a través de la interfaz de bus 154 hacia y desde un DSP específico 156 en una de las tarjetas DSP 142. A través de la interfaz de la herramienta de gestión 144, la herramienta de gestión (no representada) puede controlar la distribución de llamadas a los DSP 156. Por ejemplo, la distribución de llamadas se puede establecer de tal forma que las llamadas de entrada sean distribuidas aleatoriamente los DSP 156. Alternativamente, las llamadas desde ciertas unidades de encriptación/desencriptación 34 pueden ser encaminadas a DSP específicos 156 que soportan los mismos protocolos que las unidades 34.

Además de uno o más DSP 156, la tarjeta del DSP 142 incluye una interfaz de bus 158, un control 160 y una memoria de datos 162. La interfaz del bus 158 interrumpe el bus 146 y encamina el tráfico de llamadas del DSP desde y hacia las tarjetas de los DSP 142. En una forma de realización, la interfaz del bus 158 distribuye el tráfico de llamadas para diversos DSP 156 en la tarjeta del DSP 142 bajo el control del control 160.

Control 160 proporciona numerosas funciones de control para la tarjeta del DSP 142 e incluye lógica de unión ("glue logic") para la tarjeta del DSP. Un control de progreso de la llamada 166 maneja las operaciones de control de la llamada tales como el establecimiento de la llamada conjuntamente con el DSP 156. Aquí, el DSP 156 termina y genera señales de llamada bajo el control del control 160. En cooperación con la herramienta de gestión 144, un control de programación 168 puede controlar la programación de los DSP 156 en el centro protegido 36 o en las unidades de encriptación/desencriptación 34. El control 160 también puede proporcionar autorización de llamada de múltiples niveles para el acceso a diferentes recursos de red. Por ejemplo, servicios de larga distancia pueden estar limitados para ciertos abonados.

El DSP 156 en la tarjeta del DSP 142 está programado para llevar a cabo funciones similares a las del DSP 106 en las unidades de encriptación/desencriptación 34 descritas anteriormente. Por ejemplo, el DSP 156 interpreta y genera las señales de comunicación (por ejemplo, DTMF) recibidas desde y transmitidas a la tarjeta de la red 140, respectivamente. El DSP 156 incluye una función de módem 170 que modula y demodula las señales de salida y de entrada hacia y desde la tarjeta de red 140. Una función DES 172 encripta y desencripta las señales. Una función codificador/descodificador 174 comprime y descomprime las señales. Por ejemplo, en una forma de realización compatible con la forma de realización de la unidad de encriptación/desencriptación 34 descrita en la figura 4, el DSP 156 lleva a cabo las operaciones de autentificación de módem V.32, codificador de voz G7229A, FAXRELAY, encriptación/desencriptación DES de 56 bit y Deffie-Helman.

Las operaciones de los componentes descritos en la figura 5 se tratarán ahora con mayor detalle conjuntamente con las figuras 6A, 6B, 7A y 7B. Empezando en el bloque 200, las figuras 6A y 6B ilustran ejemplos de operaciones

de procesamiento de llamada llevadas a cabo por el centro protegido 36 para una llamada realizada por un abonado protegido a un destino inseguro (es decir, un no-abonado).

Este proceso comienza en la etapa del proceso de llamada que ocurre después del paso "pasar dígitos" descrito anteriormente conjuntamente con la figura 2. De este modo, en esta etapa, la llamada ha sido encaminada a uno de los DSP 156 en el centro protegido. Las funciones de encriptación/desencriptación 119 y 172 y las funciones de módem 121 y 170 para la llamada han sido descargadas desde la memoria flash 113 y la unidad de disco (no representada) dentro de los DSP 106 y 156 en la unidad de encriptación/desencriptación 34 (figura 4) y el centro protegido 36, respectivamente. Una conexión protegida se establece entre la unidad 34 y el centro protegido 36. Y el número de teléfono de destino ha sido recibido por el DSP 156 en el centro protegido 36.

En el bloque 302, el control 160 recibe los dígitos desde el DSP y determina si el número marcado por el abonado es válido. Por ejemplo, el control 160 compara el número de destino con descripciones del número de teléfono contenidas en una tabla (no representada) que son conocidas para satisfacer el esquema de composición de números la red. Si el número marcado no satisface el esquema de composición de números de la red, el control 160 puede enviar un requerimiento a la unidad de encriptación/desencriptación 34 de otro número de teléfono de destino. Alternativamente, el control 160 puede enviar una señal de incumplimiento a la unidad de encriptación/desencriptación 34. La unidad de encriptación/desencriptación 34 puede responder a este mensaje, por ejemplo, enviando otro número o bien enviando un mensaje de error al teléfono 22 (figura 1).

Si el número de destino es válido, en el bloque 204 el control 160 verifica el perfil del número y determina si el número de destino está asociado a otro abonado del servicio protegido (bloque 206). Esta operación se describe con mayor detalle más adelante conjuntamente con la figura 8.

En el bloque 210, el control 160 abre un nuevo puerto de salida. Esto es, se establece un canal distinto de aquél en el que fue recibida la llamada de entrada entre el DSP 156 y la PSTN 20. En el bloque 212, el control 160 llama al destino (por ejemplo, el teléfono 24) por el nuevo canal.

A continuación, en los bloques 214, 216 y 218, se establece un canal protegido entre la unidad 34 y el centro protegido 36. En el bloque 214, las funciones de codificador de voz (es decir, codificador/descodificador de voz 115 y 176) o las funciones de FAXRELAY 117 y 118 para la llamada son descargadas dentro de los DSP 106 y 156 y la unidad de encriptación/desencriptación 34 (figura 4) y el centro protegido 36, respectivamente. Después de que se establece el canal en el bloque 216, el control 160 envía el perfil de conexión a la unidad de encriptación/desencriptación 34 (bloque 218). Este perfil incluye, por ejemplo, las claves públicas 180 así como instrucciones y datos utilizados para llevar a cabo pruebas en la unidad 34. Además, en este momento el control 160 puede configurar o actualizar la unidad 34 como ha sido descrito antes en este documento. Además, en configuraciones en las cuales la unidad 34 utiliza el encaminamiento de mínimo coste, el perfil de conexión puede incluir perfiles del sistema de facturación.

Una vez ha sido establecida la conexión protegida entre el abonado y el destino inseguro (después de pasar las claves 180 y 182, como sea necesario), todas las comunicaciones en la red de acceso son encriptadas por la unidad de encriptación/desencriptación 34 y el centro protegido 36 (bloque 220).

La unidad 34 envía datos encriptados por la red de acceso al DSP 156. En el DSP 156, la función de módem 170 demodula los datos, entonces la función de DES 172 desencripta los datos demodulados. A continuación, dependiendo de si es una llamada de voz o de fax, la función de codificador de voz 176 o la función de FAXRELAY 178 que fue cargada dentro del DSP 156 (función de codificador/descodificador 174) procesa (por ejemplo, descomprime) los datos desencriptados. El DSP 156 envía los datos resultantes por el segundo canal y la red encamina estos datos al teléfono de destino.

Cuando el teléfono de destino envía información al abonado protegido, el DSP 156 recibe los datos correspondientes a través del segundo canal. Función del codificador de voz 176 o la función de FAXRELAY 178 que fue cargada dentro del DSP 156 procesa (por ejemplo, comprime) los datos y los envía a la función DES 172 la cual encripta los datos. A continuación, la función de módem 170 modula los datos encriptados y el DSP 156 envía estos datos a la unidad 34 a través del primer canal.

La sesión continúa hasta que una de las partes se desconecte (bloque 222). Si, en el bloque 223, el abonado se desconecta, se termina la llamada (bloque 224), el control 160 crea un registro de la sesión (bloque 226), entonces termina el proceso (bloque 232) hasta que se inicie la siguiente sesión.

Si, en el bloque 223, el abonado no se desconecta, el control 160 determina si está pendiente una nueva llamada (bloque 228). Si es así, el proceso procede al bloque 230 y el control 160 recupera el nuevo número de destino marcado por el abonado. Si una nueva llamada no está pendiente en el bloque 228, el proceso procede al bloque 224 y el control 160 termina la llamada como ha sido descrito antes.

Con referencia ahora a las figuras 7A y 7B, se ilustran ejemplos de operaciones de procesamiento de llamadas llevadas a cabo por el centro protegido 36 durante una llamada desde un destino inseguro a un abonado protegido empezando en el bloque 250. El proceso descrito comienza en una etapa en el proceso de la llamada que coincide con el primer paso descrito antes conjuntamente con la figura 3.

En el bloque 252, el control 160 espera una llamada entrante. El llamador no protegido llama a un abonado marcando un número de teléfono que inicia una llamada al centro protegido 36. Después de que el centro protegido 36 recibe la llamada, el control 160 recupera la información del servicio de identificación del número marcado ("DNIS" - Dialed Number Identification Service) asociada con la llamada desde el DSP 156 (bloque 254).

En el bloque 256, un traductor del número llamado 184 relaciona en correspondencia la información del DNIS con el número de teléfono real del abonado comparando el DNIS con los números de teléfono en un diagrama de abonados 186. En una forma de realización típica, el conjunto superior de dígitos en el DNIS identifica un grupo de seguimiento asociado con un centro protegido 36. De ese modo, el equipo de conmutación en la PSTN 20 (por ejemplo en la CO 26) utiliza esta información para encaminar la llamada al centro protegido 36. El traductor del número marcado 184 compara el conjunto inferior de dígitos (por ejemplo, los últimos tres o cuatro dígitos) del DNIS con las entradas del diagrama de abonados para determinar el número de teléfono de destino (esto es, el número de teléfono del abonado que está siendo llamado). El control 160 pasa este número al DSP 156 el cual inicia la llamada al abonado (bloque 258).

Como ha sido descrito anteriormente en ese documento conjuntamente con la figura 3, el control 160 recibe el progreso de la llamada desde la PSTN 20 (bloque 260) y pasa esta información de vuelta al llamador (bloque 262). En el caso de una desconexión (bloque 264) el proceso procede al bloque 266 en donde se termina la llamada. Entonces, el control 160 crea un registro de la sesión (bloque 268) y el proceso termina (bloque 269) hasta que se inicie la siguiente sesión.

Si, en el bloque 264, la llamada no se desconecta, el control 160 espera una indicación contestada desde el destino. Después de que la llamada haya sido contestada (bloque 270), el control 160 envía una señal de conexión protegida ("SC"- Secure Connection) a la unidad de encriptación/desencriptación 34 (bloque 272).

Si la unidad de encriptación/desencriptación 34 no reconoce la señal SC (bloque 274), la llamada será desconectada en el bloque 275. De otro modo, las funciones de módem 121 y 170 para la unidad 34 (figura 4) y el centro protegido 36 están sincronizadas (bloque 276) y las funciones de autentificación 123 y 190 (figuras 4 y 5) intercambien información de autentificación (bloque 278).

A continuación, el centro protegido 36 y la unidad de encriptación/desencriptación 34 cooperan para proteger la red de acceso (bloque 280). Además, cuando la conexión al abonado está siendo establecida inicialmente, el control 160 verifica el perfil y los mensajes de los abonados, como sea necesario (bloque 282).

Una vez se establece la conexión protegida entre los puntos terminales (por ejemplo, los teléfonos 22 y 24), el centro protegido procesa la llamada (por ejemplo, encripta/desencripta los datos) como ha sido expuesto anteriormente en este documento (bloque 284). Después de que haya sido completada la llamada, el proceso termina en el bloque 286 hasta que se inicie la siguiente sesión.

Los componentes del centro protegido 36 pueden ser implantados utilizando una variedad de dispositivos. Por ejemplo, como la unidad de encriptación/desencriptación 34, el DSP 156 puede ser un TMS320542PGE-2-50 de TEXAS INSTRUMENTS. La tarjeta de la red 140 puede ser una tarjeta comercialmente disponible T1, E1 o ISDN comercializada por empresas tales como DIALOGIC.

La figura 8 ilustra diversas configuraciones diferentes que pueden ser utilizadas en la implantación de la invención. Por ejemplo, las unidades de encriptación/desencriptación 34 pueden ser implantadas en un sistema de múltiples unidades 300. Esto es, el sistema de múltiples unidades incluye diversas unidades 34, implantadas utilizando uno o más DSP. Esta configuración puede ser utilizada para capacitar a que los abonados compartan los recursos de llamada protegida. Esto es deseable, por ejemplo, cuando los abonados sólo ocasionalmente realizan llamadas protegidas. En esta configuración, los terminales (por ejemplo, teléfonos, máquinas de fax, ordenadores con módem o bien otros componentes de telefonía) están conectados a un PBX 306 y pueden acceder al servicio protegido utilizando una opción soportada por el PBX 306. Si todas las unidades 34 del sistema 300 no están actualmente en uso, el PBX 306 encamina la llamada a una de las unidades 34 en el sistema 300. De ese modo, el sistema puede proporcionar servicio protegido a varios usuarios de una manera económica sobre una parte crítica de la red: la red de acceso entre el PBX 306 el PSTN 20.

En otra forma de realización, las unidades 34 pueden estar integradas dentro del CPE. Por ejemplo, las unidades 34 pueden estar implantadas como conjuntos de pastillas 307 que están integradas dentro de tarjetas de línea en el PBX 306.

La figura 8 ilustra una forma de realización de la invención en la que un centro protegido en línea 308 está instalado en la red de acceso (es decir, intercepta llamadas hacia y desde la CO). Aquí, el centro protegido en línea 308 incluye interfaces de línea apropiadas para formar interfaz con la CO 310 y el equipo en la red de acceso (por ejemplo, la unidad 312). Además, se realizan modificaciones apropiadas para la distribución de las llamadas al equipo de conmutación en la CO 310.

La figura 8 describe también diversos tipos diferentes de redes de acceso. La red de acceso puede incluir un tipo de bucle digital de abonado ("xDSL" (Digital Subscriber Loop), en donde la "x" representa diferentes tipos de DSL)

en donde las llamadas son encaminadas desde la CO 28 hacia y desde un conmutador xDSL remoto (representado por el conmutador 314) por una línea multiplexada (representada por la línea 316). El conmutador xDSL encamina entonces las llamadas hacia y desde los abonados (por ejemplo, el ordenador 318). La red de acceso también puede utilizar un sistema de distribución de fibra. En este caso, la línea 316 es una conexión de fibra óptica y el conmutador 314 es un conmutador que termina la conexión de fibra y distribuye las llamadas como antes. La red de acceso puede consistir también en un bucle local inalámbrico en el que transmisores-receptores inalámbricos apropiados 312 y 320 son utilizados entre una CO (por ejemplo, 310) y el abonado (por ejemplo, el teléfono 322).

La figura 8 ilustra también una forma de realización de la invención que proporciona conexiones protegidas terminal a terminal. Por ejemplo, los puntos terminales 304 y 318 tienen ambos asociadas unidades de encriptación/desencriptación 34. Ambas unidades 34 están programadas con el número de teléfono del centro protegido 36.

El centro protegido 36 establece un servicio terminal a terminal determinando si el destino llamado es un abonado. Con referencia otra vez a la figura 6A, en el bloque 206, el control 160 verifica las tablas de abonados 326 o 328 ubicadas en el centro protegido 36 o en una base de datos central 330. En una forma de realización, el centro protegido 36 accede a la base de datos central 330 por una conexión de Internet TCP/IP 332.

Las tablas de abonados 326 y 328 contienen listas de abonados y sus números de teléfono reales. Una tabla de abonados puede contener abonados ubicados en un área local del centro protegido 36 (por ejemplo, la tabla 326) o puede contener todos los abonados de la red (por ejemplo, la tabla 328).

Si el destino es un abonado, el control 160 (figura 5) recupera el número de teléfono del abonado (bloque 208) y establece una sesión protegida con el destino de una manera similar a la que sido expuesta antes en este documento. Una vez se establece la sesión protegida, la información enviada desde el DSP 156 a cualquier destino será encriptada.

En una forma de realización la información se encripta terminal a terminal, excepto para dentro del centro protegido. Esto es, el centro protegido 36 desencripta la información recibida desde cada unidad 34 y encripta la información enviada a cada unidad 34.

En una forma de realización alternativa, el centro protegido 36 puede deshabilitar estas operaciones de encriptación y desencriptación y simplemente pasa los datos encriptados a los dos puntos terminales. Esto se puede conseguir, por ejemplo, configurando las tarjetas de la red 140 para encaminar el tráfico de llamadas directamente desde un canal a otro canal, saltando la tarjeta del DSP 142. En este caso, sin embargo, la tarjeta del DSP 142 todavía proporciona el establecimiento inicial de la llamada, pasando las claves y otras operaciones para ayudar a los puntos terminales en el establecimiento de la conexión. Además, la tarjeta del DSP 142 puede supervisar la conexión.

Otras configuraciones que incorporan las enseñanzas de la invención pueden ser comprendidas mediante una referencia adicional a la figura 8. Por ejemplo, conferencias protegidas entre más de dos participantes pueden estar provistas encaminando las llamadas a través de único centro protegido 36. El centro protegido 36 puede ser conectado (tanto directamente como indirectamente) a cualquier nodo en la PSTN. De este modo, los centros protegidos 36 pueden estar distribuidos a través de la PSTN 20 para proporcionar el nivel deseado de servicios de llamadas protegidas.

La figura 8 ilustra también una estación de gestión 334 utilizada para gestionar el sistema. La estación de gestión 334 y el centro protegido 36 proporcionan ambos interfaces de integración de telefonía e informática ("CTI"). El centro protegido 36 puede estar configurado y gestionado desde la estación de gestión 334 a través, por ejemplo, de una conexión TCP/IP o X.25 (línea 335). Esto incluye, por ejemplo, gestión de base de datos, gestión de claves, recogida y grabación de audio, gestión de la información del perfil del usuario y supervisión del comportamiento.

Con referencia a las figuras 9A y 9B, se representa una forma de realización de la invención que soporta terminales de la ISDN BRI y canales de la ISDN PRI. Un abonado que utilice un equipo terminal de la ISDN ("TE" - Terminal Equipment) 340 establece una llamada a un intercambio local (designado por "LT") 342 en la red 20 a través de una unidad de encriptación/desencriptación de la ISDN 344 y una terminal de red 1 ("NT1") 346. De acuerdo con la invención, un centro protegido 348 (configurado con tarjetas ISDN tal como ha sido descrito antes) coopera con la unidad de encriptación/desencriptación de la ISDN 344 para establecer una llamada protegida por la red de acceso (representada por la línea 350).

Los componentes se comunican por las interfaces definidas por la ISDN. El TE 340 y la unidad de encriptación/desencriptación de la ISDN 344 se comunican por la interfaz de cuatro cables de la ISDN S 352. La unidad de encriptación/desencriptación 344 se comunica con la NT1 346 por una interfaz de cuatro cables T 354. La interfaz T 354 es un subconjunto de la interfaz S 352. La NT1 346 marca el punto en el cual termina la red pública 20 y empiezan las instalaciones de los clientes 355. La NT1 346 proporciona una conversión en la capa física entre la interfaz T 354 y la interfaz U 350 que se conecta al intercambio local 342.

La unidad de encriptación/desencriptación de la ISDN 344 incluye dos interfaces: una para el lado del TE y otra para el lado de la NT1. La interfaz del lado del TE 356 proporciona la emulación de la NT1. La interfaz del lado de la NT1 358 proporciona la emulación del TE.

La unidad de encriptación/desencriptación de la ISDN 344 incluye un procesador 360 y lleva a cabo la función de encriptación/desencriptación 362, codificación y otras funciones que son similares a aquellas llevadas a cabo por el DSP descritas antes en este documento. La unidad 344 encripta/desencripta los dos canales B de la señal de la BRI pero no encripta el canal D. La unidad 344 lleva a cabo también las funciones de señalización tales como Q.931 o Q.921.

La unidad de encriptación desencriptación de la ISDN 344 incluye también dispositivos de memoria de datos 364 y 366, lógica de unión 371 y un componente de copia de seguridad de encriptación del DSP 367 que coopera para soportar la capacidad de programación de la unidad 344 y proporcionar otras funciones. Debe comprenderse que, como en un sistema electrónico típico, la lógica de unión descrita en las formas de realización anteriores puede servir para conectar algunos o todos los componentes en la respectiva unidad. Muchos de los componentes anteriores así como de los dispositivos de entrada y de salida (por ejemplo, LCD 371) y otros circuitos (no representados) llevan a cabo funciones similares a las de los componentes descritos conjuntamente con la figura 4. De acuerdo con ello, algunos componentes de los equipos similares y programas de software pueden ser utilizados en las dos formas de realización.

La unidad de encriptación/desencriptación de la ISDN 344 puede estar construida utilizando una variedad de dispositivos. Por ejemplo, las interfaces pueden estar implantadas utilizando pastillas MC145574PB S/T INTERFACE comercializadas por MOTOROLA. El procesador puede ser implantado utilizando uno de los controles Quad Integrated Communications Controllers comercializados por Motorola. El procesador puede comunicar con la interfaz a través de una interfaz general de circuito ("GCI") 365.

Las figuras 9A y 9B ilustran también un dispositivo de encriptación/desencriptación de múltiples unidades 370 que forma interfaz con una conexión PRI ISDN 372. Como es conocido en la técnica, la conexión PRI ISDN puede ser transportada por una línea El (30B + D) o una línea T1 (24B + D). En una forma de realización, el dispositivo 370 incluye diversas unidades de encriptación/desencriptación PRI ISDN 374. En una forma de realización alternativa (no representada), los componentes de los encuadradores 376 y 378 (por ejemplo, el procesador 360, etcétera) pueden estar alojados en unidades separadas que se conectan al dispositivo 370 a través de un canal representado por la línea 380. Por ejemplo, un canal PRI ISDN puede estar separado dentro de cada uno de sus canales de la BRI. Cada uno de los canales de la BRI, a su vez, puede ser conectado entonces a la correspondiente unidad de encriptación/desencriptación a través de una línea física.

Las funciones de los encuadradores 376 y 378 son formar interfaz de un único canal con los canales PRI multiplexados. El encuadrador y la interfaz de línea 376 empiezan y terminan la línea E1 o la línea T1. Esto incluye la detección y la generación del encuadrado apropiado para la línea. El encuadrador E1/T1 demultiplexa y multiplexa un único canal (por ejemplo, un canal de la BRI) desde y sobre la conexión PRI ISDN, respectivamente.

El canal único se conecta a un procesador 360 que proporciona funciones de encriptación y desencriptación 362 y funciones de señalización 368. En el otro lado del procesador 360 el canal se conecta a un equipo terminal de la ISDN (no representado) a través de una interfaz de línea 356. Para reducir la complejidad de la figura 9, el resto de los componentes en la unidad 374 (por ejemplo, una copia de seguridad de la encriptación del DSP 367, lógica de unión 369, memoria de datos 364, memoria flash 366 y LCD 371) no se ilustran. Debe entenderse que estos componentes pueden llevar a cabo funciones similares a las descritas antes en este documento conjuntamente con la unidad de encriptación/desencriptación ISDN 344 expuesta en la figura 8.

A partir de lo anterior, se verá que la invención proporciona un sistema de protección eficaz para aplicaciones de telefonía. Este sistema puede proteger la conexión sin que se requiera intervención por parte del abonado. El equipo de encriptación/desencriptación basado en la red determina automáticamente si la llamada es hacia o desde una parte protegida y establece una llamada protegida de acuerdo con ello.

El sistema proporciona también protección terminal a terminal cuando todas las partes tienen equipo de encriptación/desencriptación. De nuevo, la conexión protegida se puede establecer automáticamente, sin ayuda por parte de los abonados.

El sistema reduce las posibilidades de que una persona que realice una escucha ilegal rastree una llamada porque un abonado siempre llama a un centro protegido. El número de teléfono de destino real sólo se pasa después de que la línea esté protegida.

Además, la invención reduce la posibilidad de la supervisión por parte del proveedor del servicio de teléfono debido a que los números de teléfono de la fuente y de destino no se pasan por la red. En cambio, las llamadas hacia y desde el abonado, en efecto, están escondidas por el terminal frontal del centro protegido.

Mientras ciertas formas de realización específicas de la invención han sido expuestas como típicas, la invención no está limitada a esas formas particulares, sino que en cambio se puede aplicar ampliamente a todas aquellas variaciones que quedan dentro del ámbito de las reivindicaciones. A aquellos expertos en la técnica a la cual pertenece la invención se les ocurrirá diversas modificaciones y adaptaciones. Por ejemplo, se pueden utilizar diversos procedimientos de encriptación de datos en la puesta en práctica de la invención. Una serie de procedimientos pueden ser utilizados para encaminar las llamadas hacia o desde un centro protegido o para llevar a cabo otras operaciones relacionadas de

encaminamiento de la llamada. También, la invención puede ser implantada utilizando una variedad de componentes de equipos conjuntamente con algoritmos de software apropiados. Por lo tanto, las estructuras y los procedimientos específicos expuestos en detalle anteriormente en este documento son meramente ilustrativos de unas pocas formas de realización específicas de la invención.

REIVINDICACIONES

1. Procedimiento para proporcionar comunicaciones protegidas en una red de telefonía, en el que la red proporciona la conectividad para las comunicaciones entre una pluralidad de instalaciones de los clientes y en el que la red incluye una pluralidad de nodos de conmutación para proporcionar la conectividad, **caracterizado** porque el procedimiento comprende los pasos de:

establecer automáticamente (50, 52) una conexión (38) entre el primero de los equipos de las instalaciones de los clientes (22) y un aparato de encriptación y desencriptación (34);

establecer (53, 56, 58) una conexión encriptada (30, 44) entre un centro protegido (36) y el aparato de encriptación y desencriptación (34);

proteger la conexión establecida entre el aparato de encriptación y desencriptación (34) y el centro protegido (36); y

enviar (66) información del destino por la conexión protegida.

2. El procedimiento de la reivindicación 1 en el que el aparato de encriptación y desencriptación está instalado en un nodo de conmutación.

3. El procedimiento de la reivindicación 1 o la reivindicación 2 adicionalmente comprendiendo el paso de la distribución de las comunicaciones para una pluralidad de equipos de instalaciones de los clientes a una pluralidad de procesos de encriptación y desencriptación que se ejecutan en el aparato de encriptación y desencriptación.

4. El procedimiento de cualquiera de las reivindicaciones anteriores en el que el paso de protección incluye la combinación de la conexión protegida y de la conexión establecida entre el centro protegido y el aparato de encriptación y desencriptación en una única conexión.

5. El procedimiento de cualquiera de las reivindicaciones anteriores en el que el paso de protección comprende el encaminamiento de las comunicaciones entre la conexión protegida y la conexión establecida entre el centro protegido y el aparato de encriptación y desencriptación.

6. El procedimiento de cualquiera de las reivindicaciones anteriores en el que el paso del establecimiento de la conexión entre el centro protegido y el aparato de encriptación y desencriptación adicionalmente comprende el paso de la iniciación de una llamada telefónica utilizando un primer número de teléfono asociado a un abonado; y el paso del establecimiento de la conexión entre dicho primer equipo de las instalaciones de los clientes (22) y dicho aparato de encriptación y desencriptación (34) adicionalmente comprende el paso de relacionar en correspondencia el primer número de teléfono con el segundo número de teléfono e iniciar una llamada de teléfono al abonado utilizando el segundo número de teléfono.

7. El procedimiento de cualquiera de las reivindicaciones anteriores adicionalmente comprendiendo el paso del establecimiento de una conexión al aparato de encriptación y desencriptación utilizando un número por defecto asociado con el aparato de encriptación y desencriptación.

8. El procedimiento de la reivindicación 7 adicionalmente comprendiendo el paso del almacenaje del número por defecto en una memoria de datos.

9. El procedimiento de cualquiera de las reivindicaciones anteriores adicionalmente comprendiendo los pasos del establecimiento de una conexión protegida de voz, fax y datos entre el aparato de encriptación y desencriptación (34) y el centro protegido (36).

10. El procedimiento de cualquiera de las reivindicaciones anteriores adicionalmente comprendiendo el paso del establecimiento de una conexión entre el aparato de encriptación y desencriptación y un lado del nodo de la red de una red de acceso y el equipo de las instalaciones de los clientes.

11. El procedimiento de la reivindicación 10 adicionalmente comprendiendo los pasos de proporcionar una pluralidad de aparatos de encriptación y desencriptación en por lo menos un lado de las instalaciones de los clientes de una red de acceso; y la distribución de las comunicaciones para la pluralidad de aparatos de encriptación y desencriptación a una pluralidad de procesos de encriptación y desencriptación que se ejecutan en el aparato de encriptación y desencriptación en un lado del nodo de la red de una red de acceso.

12. El procedimiento de la reivindicación 11 en el que el aparato de encriptación y desencriptación en un lado del nodo de la red de una red de acceso está instalado en un intercambio local.

13. El procedimiento de la reivindicación 1 en el que el paso de la protección de la conexión establecida entre el aparato de encriptación y desencriptación (34) y el centro protegido (36) adicionalmente comprende:

la autentificación de dicho aparato de encriptación y desencriptación (34) por dicho centro protegido sobre dicha conexión encriptada;

la encriptación por dicho aparato de encriptación y desencriptación (34) señalando el origen en dicho equipo de las instalaciones de los clientes (22); y

la encriptación por dicho aparato de encriptación y desencriptación (34) de las comunicaciones originadas en dicho equipo de las instalaciones de los clientes (22).

14. El procedimiento de la reivindicación 1 en el que el paso de la protección de la conexión establecida entre el aparato de encriptación y desencriptación (34) y el centro protegido (36) adicionalmente comprende:

la encriptación de las comunicaciones de salida incluyendo la señalización (62, 66, 68, 70) requerida para el establecimiento de dicha conectividad;

el envío de las comunicaciones de salida encriptadas por una red de acceso (30, 44);

la desencriptación de las comunicaciones de salida en un centro protegido el cual está conectado a uno de dichos nodos de conmutación;

la encriptación de las comunicaciones de entrada incluyendo la señalización (92, 93) requerida para el establecimiento de dicha conectividad en dicho centro protegido;

el envío (94, 95) de las comunicaciones de entrada encriptadas por una red de acceso; y

la desencriptación de las comunicaciones de entrada recibidas por una red de acceso.

15. El procedimiento de cualquiera de las reivindicaciones anteriores en el que dicho centro protegido está instalado en un intercambio local.

16. El procedimiento de cualquiera de las reivindicaciones anteriores en el que dicho centro protegido es una plataforma de interfaz de ordenador y telefonía.

17. El procedimiento de la reivindicación 14 adicionalmente comprendiendo el paso del envío de las comunicaciones de salida desencriptadas al equipo de las instalaciones de los clientes.

18. El procedimiento de la reivindicación 14 adicionalmente comprendiendo el paso de la recepción de las comunicaciones de entrada desde el equipo de las instalaciones de los clientes.

19. El procedimiento de la reivindicación 1 en el que el paso de la protección de la conexión establecida entre el aparato de encriptación y desencriptación (34) y el centro protegido (36) adicionalmente comprende:

la encriptación de las comunicaciones de salida incluyendo la señalización (62, 66, 68, 70) requerida para el establecimiento de dicha conectividad;

el envío de las comunicaciones de salida encriptadas por una red de acceso (30, 44);

la desencriptación de las comunicaciones de salida en un centro protegido (36) el cual está conectado a uno de dichos nodos de conmutación; y

el envío de la salida desencriptada a un teléfono (24).

20. El procedimiento de la reivindicación 1 adicionalmente comprendiendo el establecimiento de una conexión protegida de voz, fax y datos entre una primera y una segunda instalación de los clientes (40).

21. Un sistema para proporcionar comunicaciones seguras por una red de telefonía **caracterizado** porque el sistema comprende:

un primer aparato de encriptación y desencriptación (34) para establecer automáticamente y para mantener una conexión encriptada de un equipo de las instalaciones de los clientes (22) que comprende:

por lo menos una interfaz de la red del teléfono (100) para iniciar y terminar una pluralidad de llamadas de teléfono hacia y desde una pluralidad de aparatos de encriptación y desencriptación de las instalaciones de los clientes (34), respectivamente;

por lo menos un procesador de encriptación y desencriptación (106) para encriptar y desencriptar comunicaciones que incluyen voz, fax, datos y una combinación simultánea de cualquiera de ellos, voz, fax y datos;

una memoria de datos (128) integrada dentro de dicho procesador para almacenar un número de teléfono asociado con un centro protegido (36);

un control de llamada integrado centro de dicho procesador para establecer una conexión protegida a un centro protegido (36) utilizando el número del teléfono almacenado; y

una pluralidad de unidades del centro protegido (36) comprendiendo:

por lo menos una interfaz de la red de teléfonos (140) para iniciar y terminar una llamada de teléfono hacia y desde el primer aparato de encriptación y desencriptación (34) y para iniciar y terminar comunicaciones hacia y desde la red pública de teléfonos conmutados PSTN (20), respectivamente; y

un procesador de encriptación y desencriptación (156) para encriptar y desencriptar comunicaciones incluyendo voz, fax, datos y una combinación de cualquiera de ellos, voz, fax y datos.

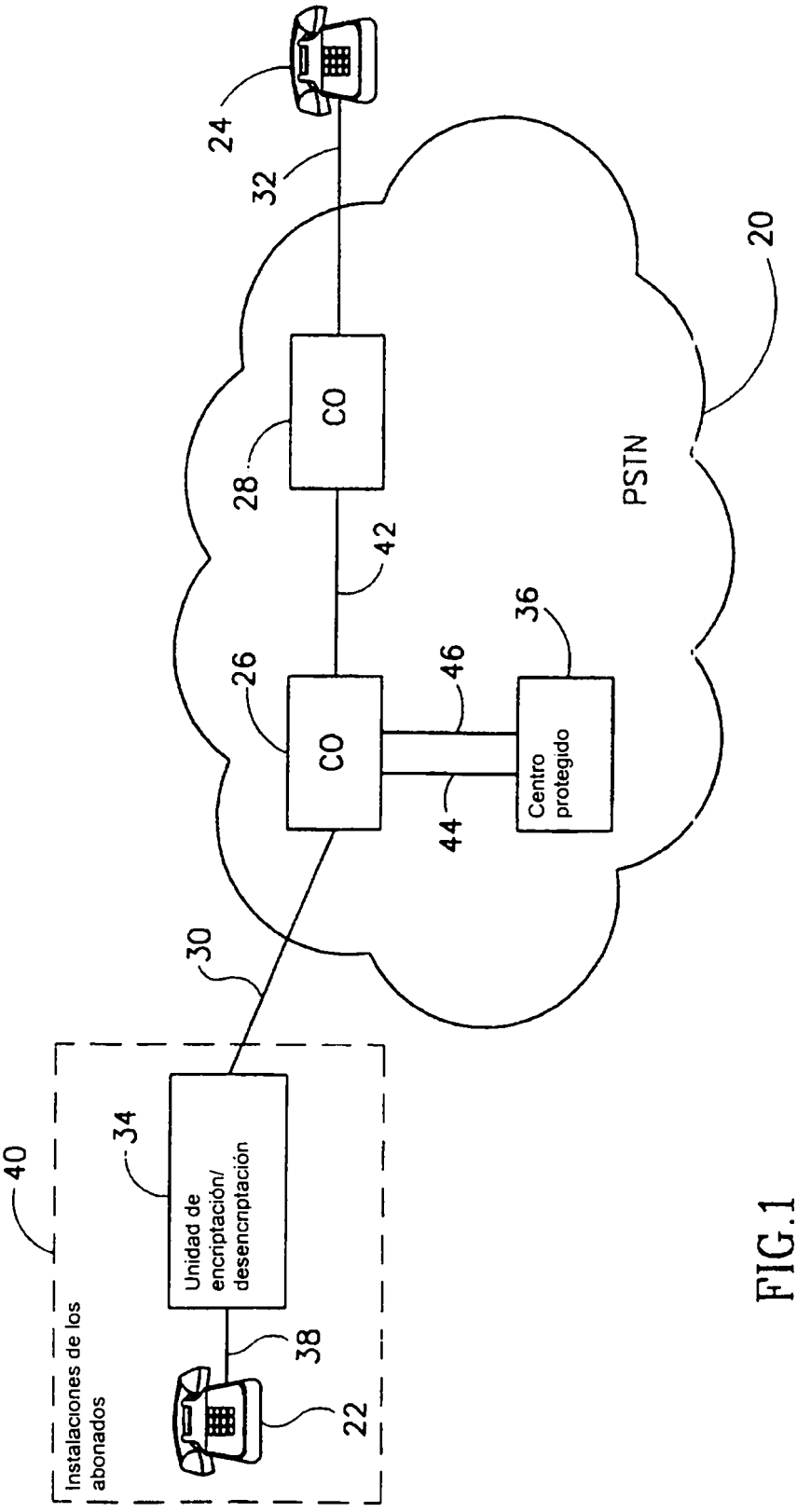

24
32
20
PSTN
CO
28
42
36
26
46
CO
Centro protegido
44
30
40
34
Unidad de encriptación/ desencriptación
Instalaciones de los abonados
38
22

FIG.1

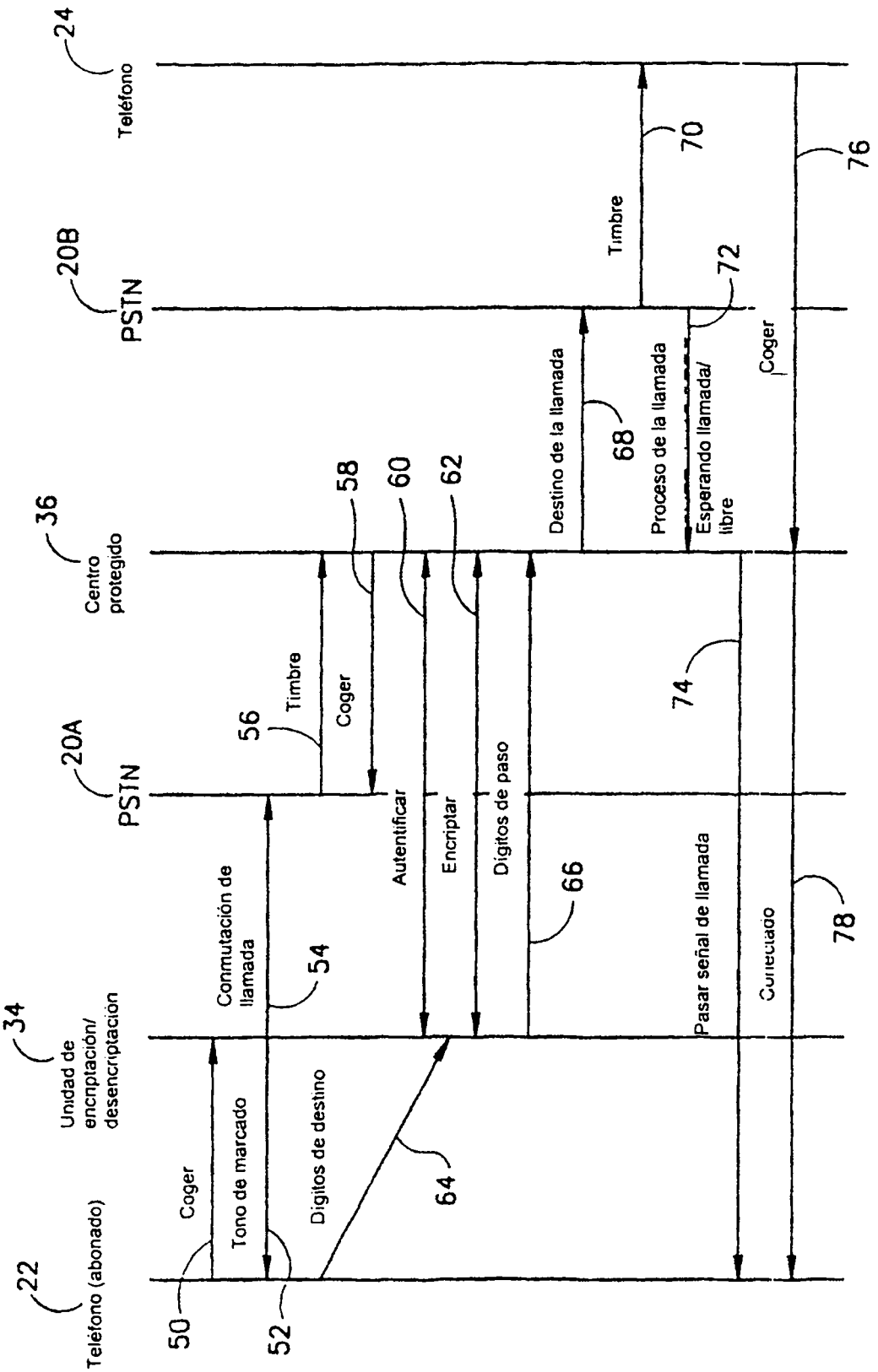

22
Teléfono (abonado)
34
Unidad de encriptación/ desencriptación
36
Centro protegido
20A
PSTN
20B
PSTN
24
Teléfono
Coger
Tono de marcado
Dígitos de destino
Conmutación de llamada
Timbre
Coger
Autentificar
Encriptar
Dígitos de paso
Destino de la llamada
Timbre
Proceso de la llamada
Esperando llamada/ libre
Coger
Pasar señal de llamada
Conectado
50
52
54
56
58
60
62
64
66
68
70
72
74
76
78

FIG.2

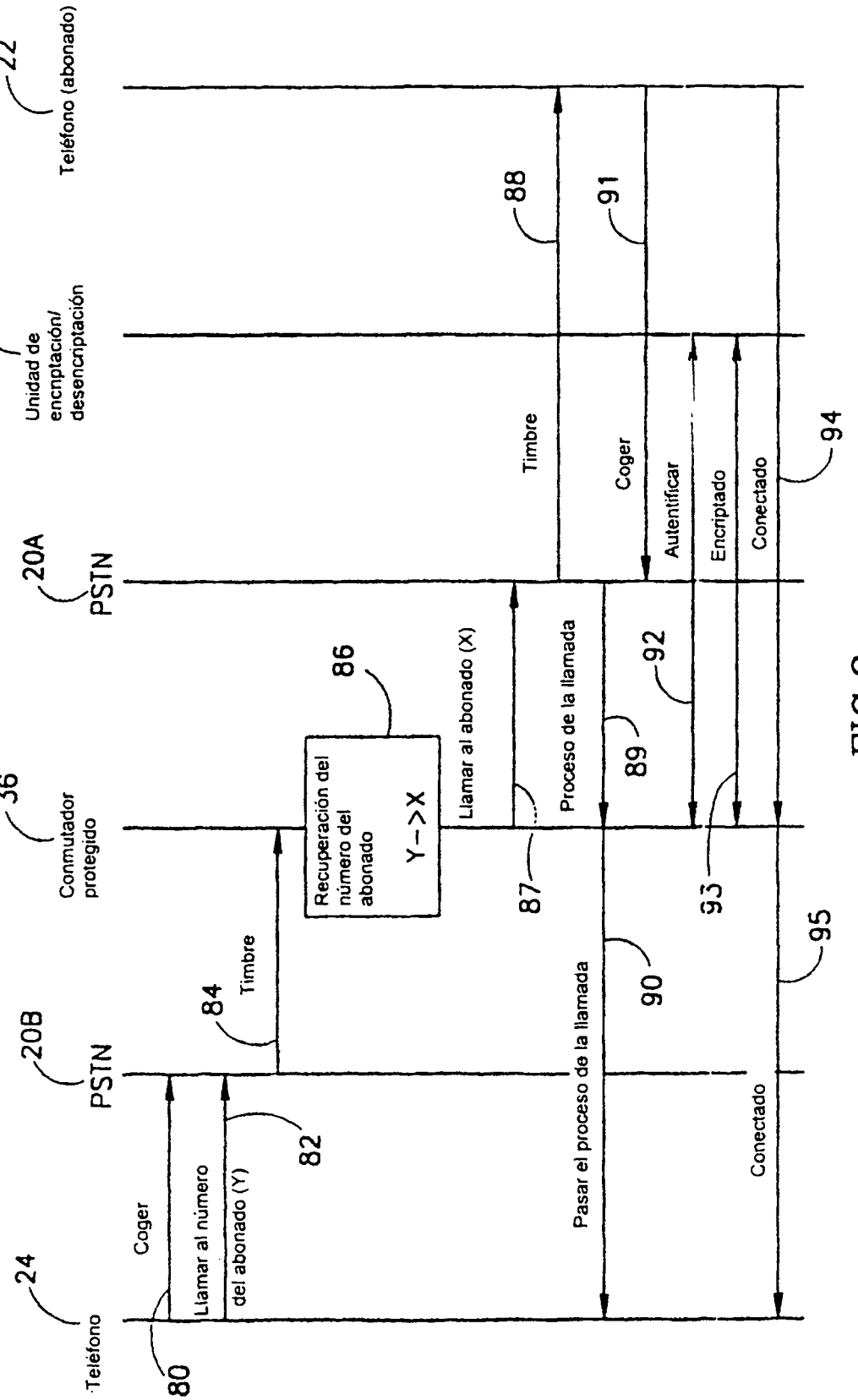
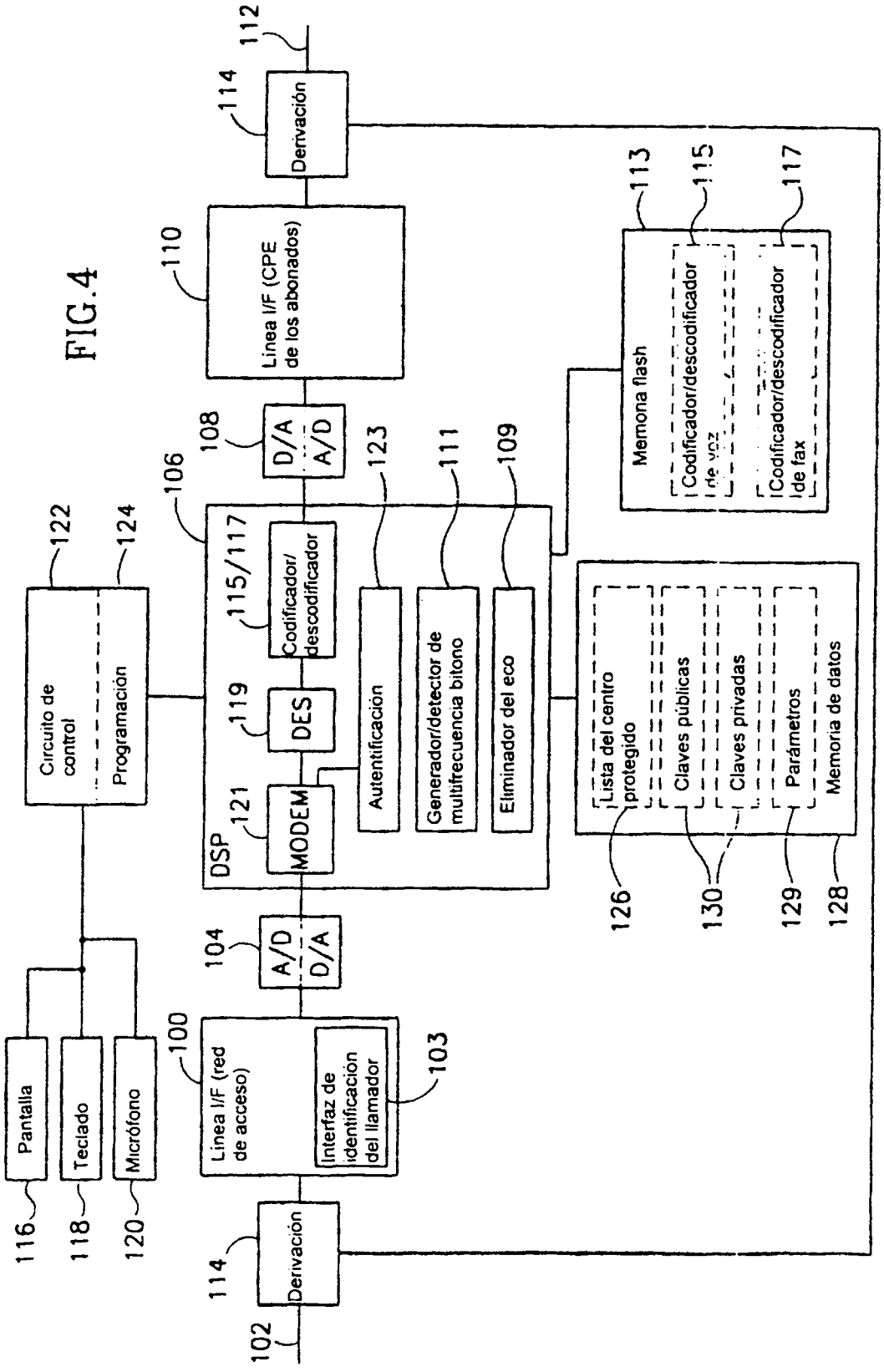

24
Teléfono
80
Coger
Llamar al número del abonado (Y)
82
20B
PSTN
84
Timbre
36
Conmutador protegido
Recuperación del número del abonado
Y->X
86
Llamar al abonado (X)
87
20A
PSTN
34
Unidad de encriptación/ desencriptación
22
Teléfono (abonado)
Timbre
88
Proceso de la llamada
89
Pasar el proceso de la llamada
90
Coger
91
Autentificar
92
Encriptado
93
Conectado
94
Conectado
95

FIG.3

FIG.4


Pantalla
Teclado
Micrófono
Circuito de control
Programación
Línea I/F (red de acceso)
Interfaz de identificación del llamador
A/D
D/A
DSP
MODEM
DES
Codificador/ descodificador
Autentificación
Generador/detector de multifrecuencia bitono
Eliminador del eco
D/A
A/D
Línea I/F (CPE de los abonados)
Derivación
Derivación
Memona flash
Codificador/descodificador
Codificador/descodificador de fax
Lista del centro protegido
Claves públicas
Claves privadas
Parámetros
Memoria de datos
100
102
103
104
106
108
109
110
111
112
113
114
115/117
116
118
119
120
121
122
123
124
126
128
129
130

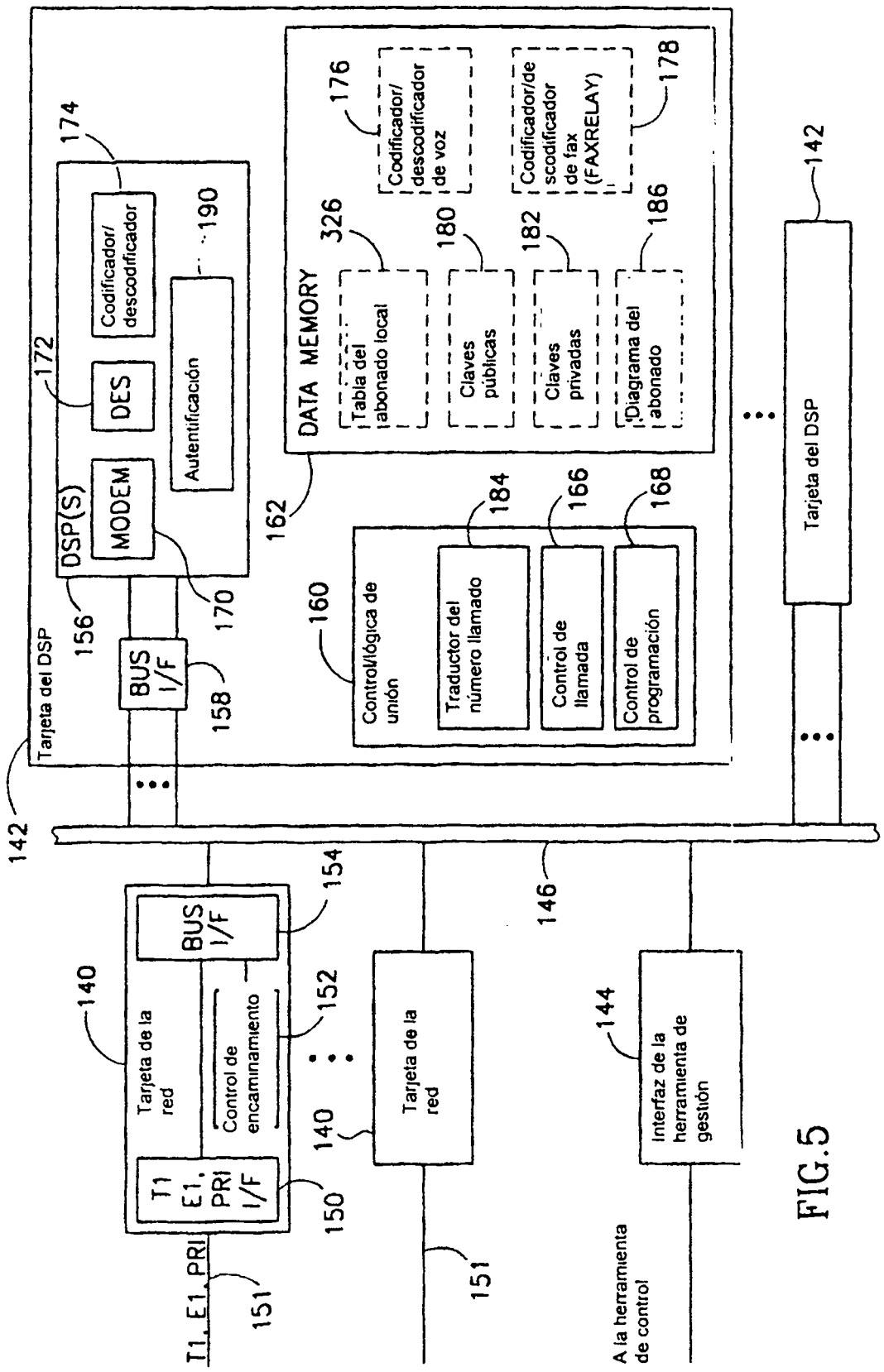

Tarjeta del DSP
142
DSP(S)
174
172
MODEM
DES
Codificador/ descodificador
Autentificación
190
156
170
BUS I/F
158
162
DATA MEMORY
326
Tabla del abonado local
180
Claves públicas
182
Claves privadas
186
Diagrama del abonado
176
Codificador/ descodificador de voz
178
Codificador/de scodificador de fax (FAXRELAY)
160
Control/lógica de unión
184
Traductor del número llamado
166
Control de llamada
168
Control de programación
Tarjeta del DSP
142
146
154
BUS I/F
140
Tarjeta de la red
Control de encaminamiento
152
T1 E1, PRI I/F
150
T1, E1, PRI
151
140
Tarjeta de la red
151
144
Interfaz de la herramienta de gestión
A la herramienta de control

FIG.5

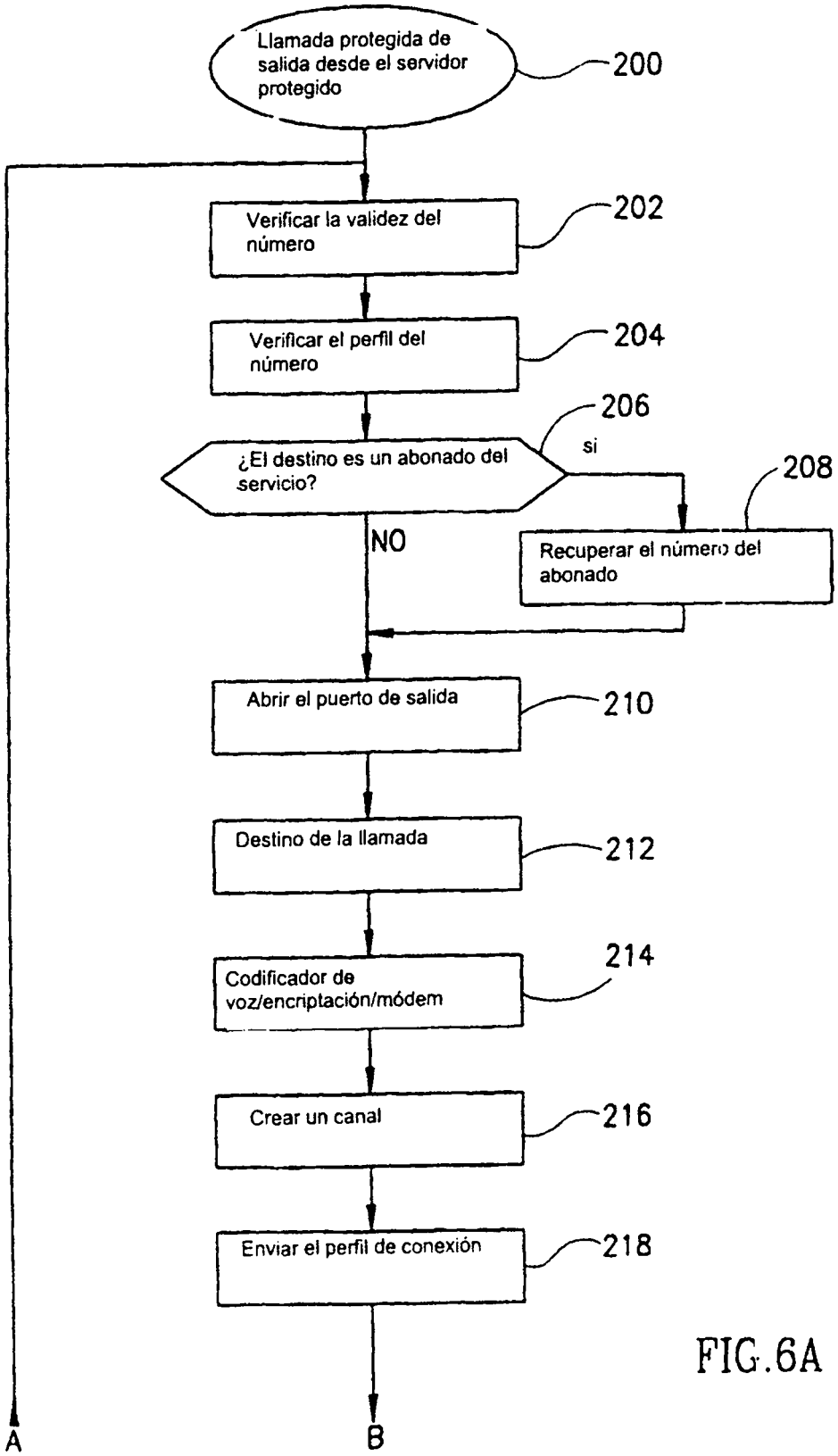

Llamada protegida de salida desde el servidor protegido
200
Verificar la validez del número
202
Verificar el perfil del número
204
¿El destino es un abonado del servicio?
206
si
208
NO
Recuperar el número del abonado
Abrir el puerto de salida
210
Destino de la llamada
212
Codificador de voz/encriptación/módem
214
Crear un canal
216
Enviar el perfil de conexión
218
A
B

FIG.6A

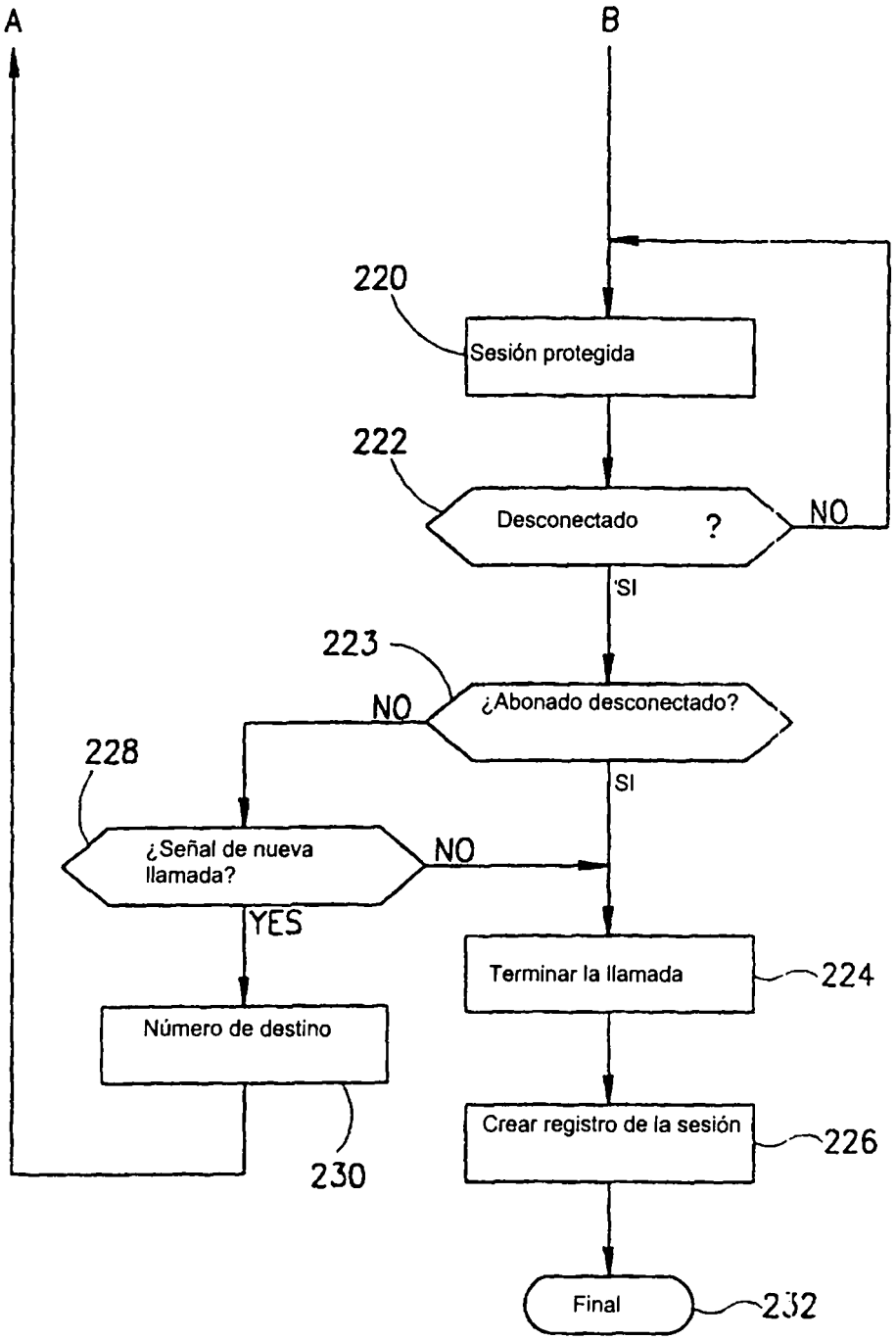

A
B
220
Sesión protegida
222
Desconectado ?
NO
SI
223
¿Abonado desconectado?
NO
SI
228
¿Señal de nueva llamada?
NO
YES
Terminar la llamada
224
Número de destino
Crear registro de la sesión
226
230
Final
232

FIG.6B

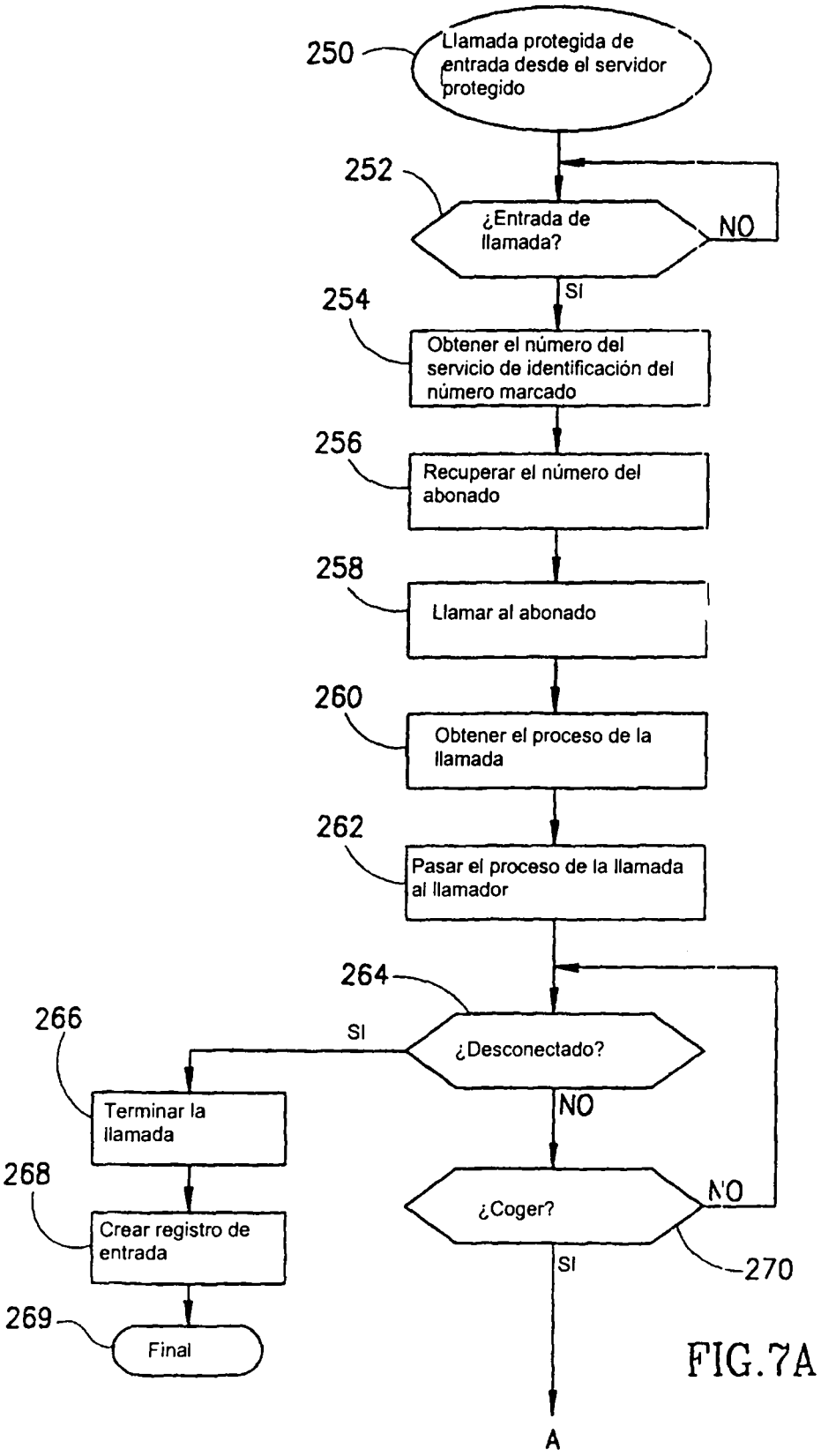

250
Llamada protegida de entrada desde el servidor protegido
252
¿Entrada de llamada?
NO
SI
254
Obtener el número del servicio de identificación del número marcado
256
Recuperar el número del abonado
258
Llamar al abonado
260
Obtener el proceso de la llamada
262
Pasar el proceso de la llamada al llamador
264
¿Desconectado?
SI
266
Terminar la llamada
NO
¿Coger?
NO
268
Crear registro de entrada
SI
270
269
Final
A

FIG.7A

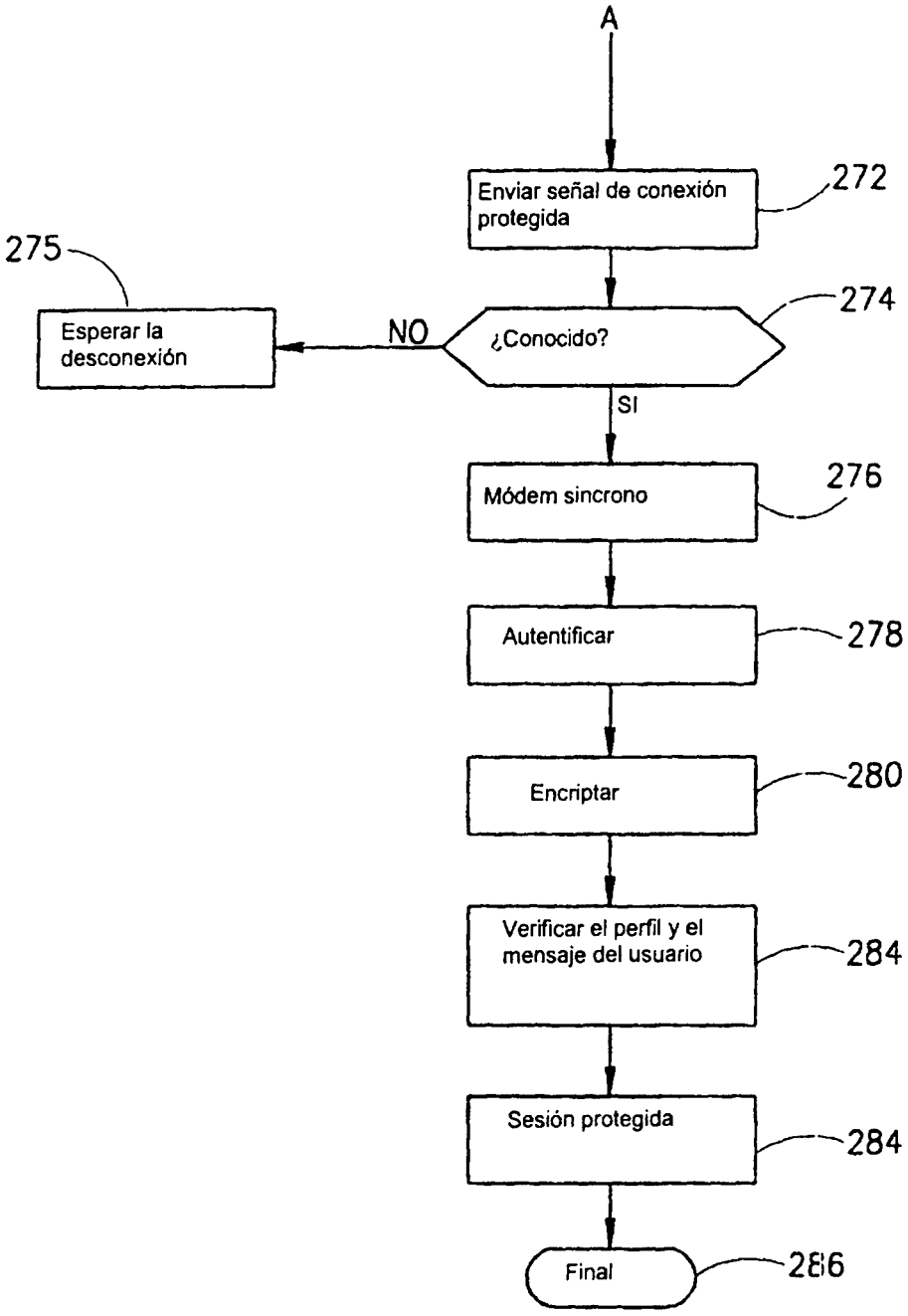

A
Enviar señal de conexión protegida
272
275
Esperar la desconexión
NO
¿Conocido?
274
SI
Módem sincrono
276
Autentificar
278
Encriptar
280
Verificar el perfil y el mensaje del usuario
284
Sesión protegida
284
Final
286

FIG.7B

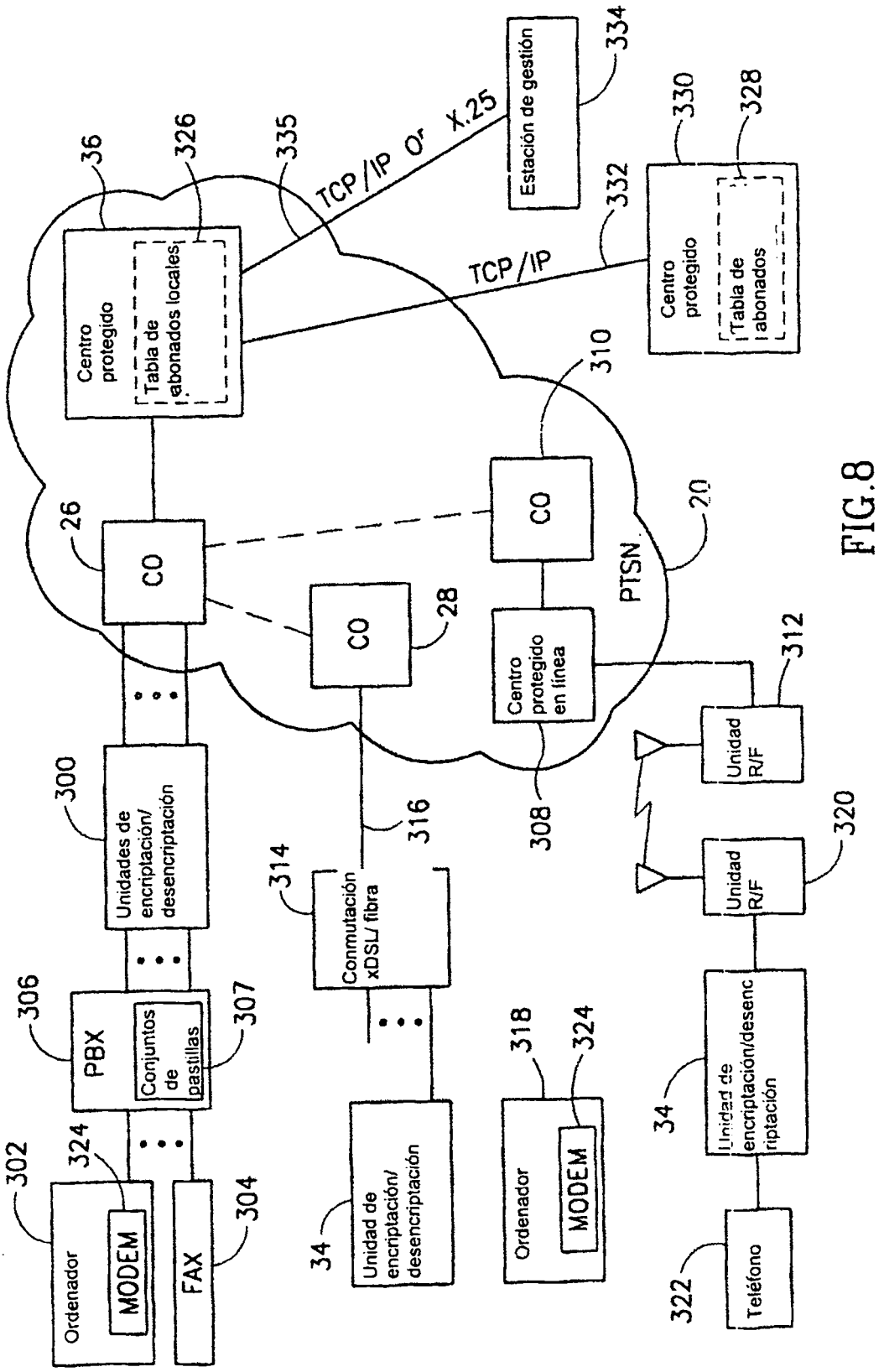

Ordenador
MODEM
FAX
PBX
Conjuntos de pastillas
Unidades de encriptación/ desencriptación
CO
CO
CO
Centro protegido
Tabla de abonados locales
Centro protegido en línea
Conmutación xDSL/ fibra
Unidad de encriptación/ desencriptación
Ordenador
MODEM
Unidad R/F
Unidad R/F
Unidad de encriptación/desencriptación
Teléfono
Centro protegido
Tabla de abonados
Estación de gestión
TCP/IP
TCP/IP o X.25
PTSN
302
304
306
307
324
300
26
28
36
326
335
310
308
316
314
318
324
34
312
320
34
322
332
330
328
334
20

FIG.8

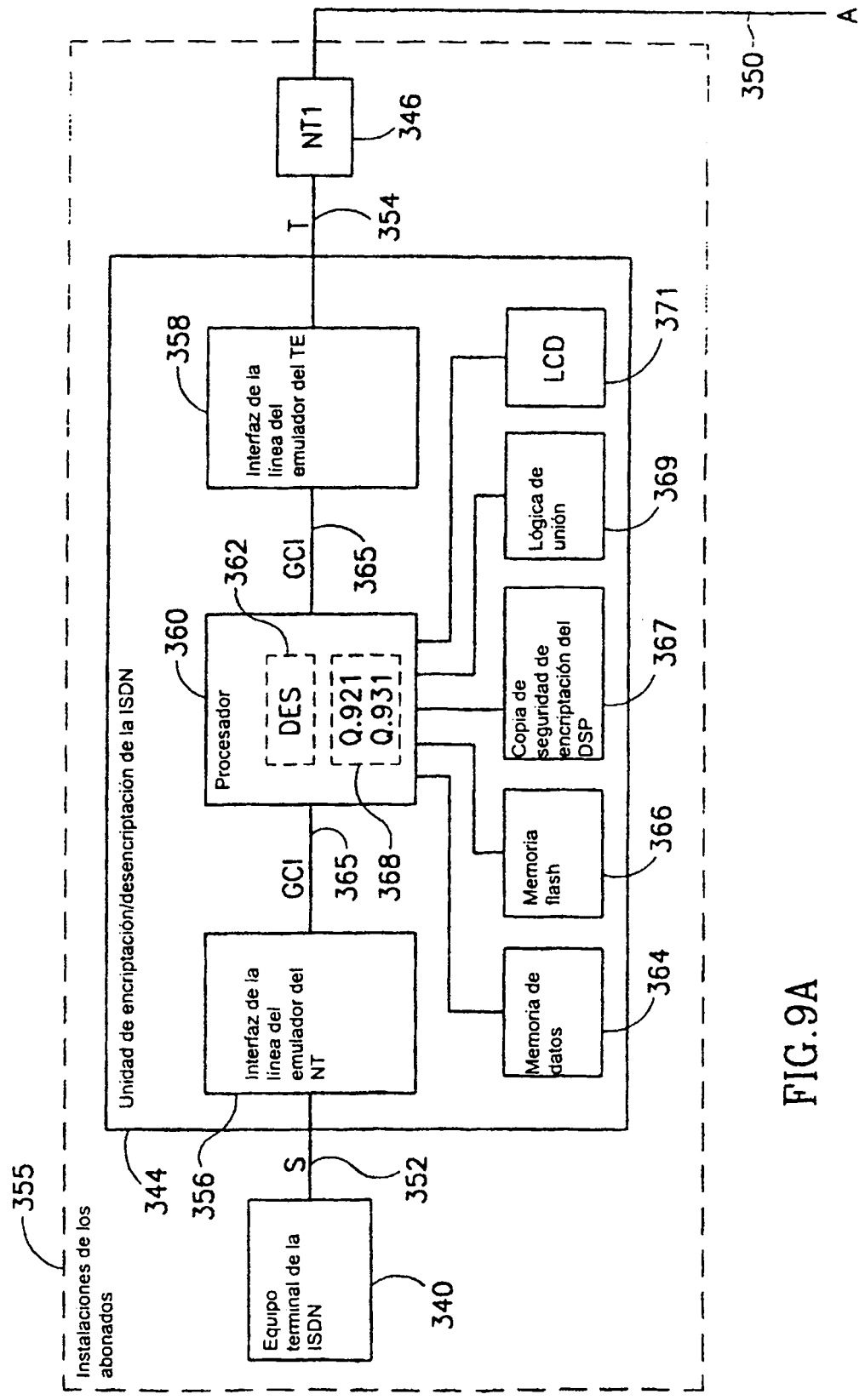

A
350
NT1
346
T
354
Unidad de encriptación/desencriptación de la ISDN
358
Interfaz de la línea del emulador del TE
LCD
371
Lógica de unión
369
GCI
365
362
360
Procesador
DES
Q.921
Q.931
Copia de seguridad de encriptación del DSP
367
GCI
365
368
Memoria flash
366
Interfaz de la línea del emulador del NT
Memoria de datos
364
S
344
356
352
355
Instalaciones de los abonados
Equipo terminal de la ISDN
340

FIG.9A

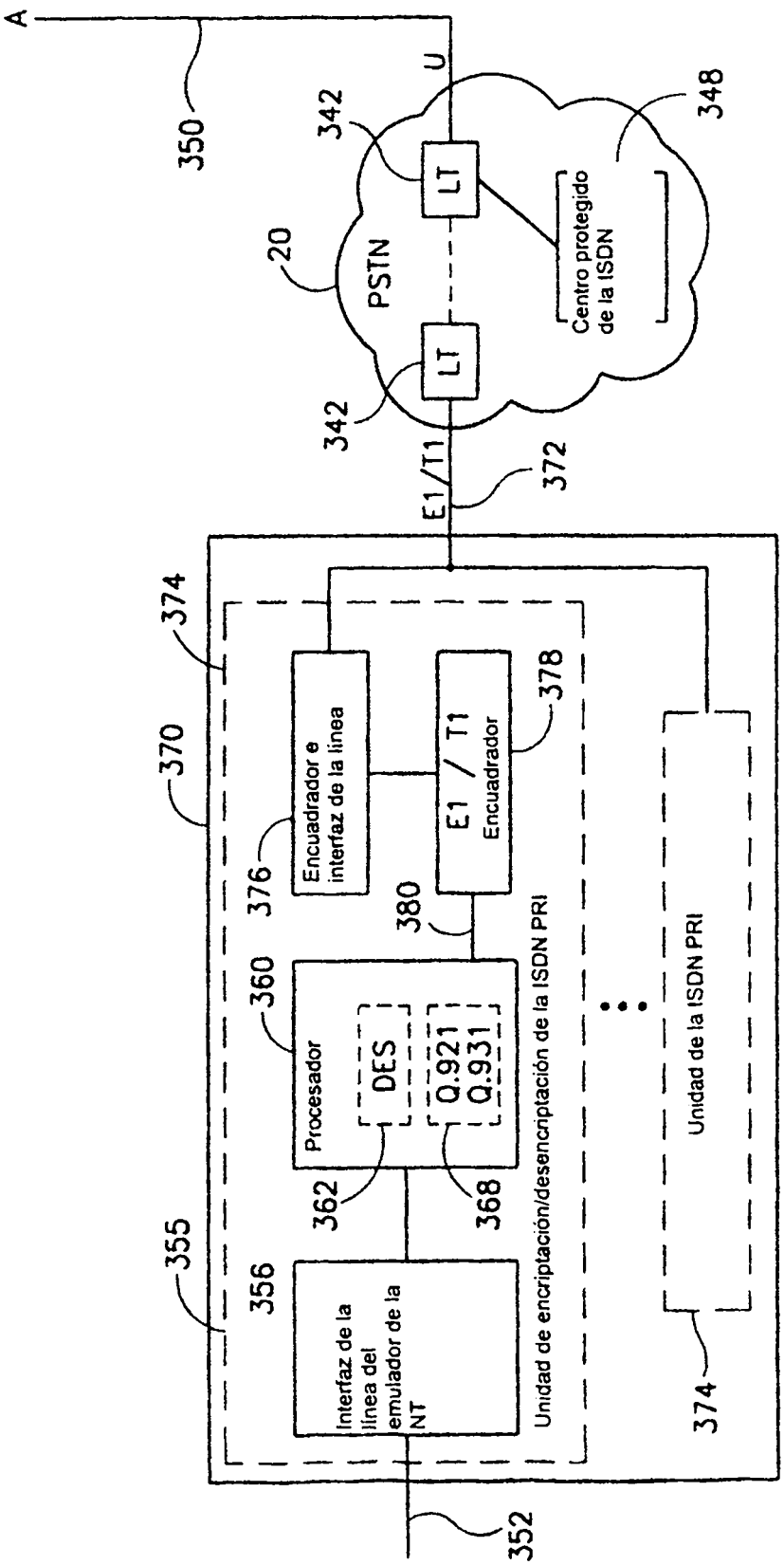

A
350
U
342
LT
348
20
PSTN
Centro protegido de la ISDN
342
LT
E1/T1
372
374
370
Encuadrador e interfaz de la línea
376
E1 / T1 Encuadrador
378
380
360
Procesador
DES
Q.921
Q.931
362
368
355
356
Interfaz de la línea del emulador de la NT
Unidad de encriptación/desencriptación de la ISDN PRI
Unidad de la ISDN PRI
374
352

FIG.9B