(19) OFICINA ESPAÑOLA DE PATENTES Y MARCAS

ESPAÑA

(11) Número de publicación: **2 553 445**

(51) Int. CI.:

***H04L 12/28*** (2006.01)

(12) TRADUCCIÓN DE PATENTE EUROPEA T3

(96) Fecha de presentación y número de la solicitud europea: **22.10.2010 E 10773609 (2)**

(97) Fecha y número de publicación de la concesión europea: **07.10.2015 EP 2529511**

(54) Título: **Procedimiento y dispositivo para controlar un sistema de automatización doméstica**

(30) Prioridad:

**25.01.2010 DE 102010005756**

(45) Fecha de publicación y mención en BOPI de la traducción de la patente:
**09.12.2015**

(73) Titular/es:

**RWE EFFIZIENZ GMBH (50.0%)**
**Flamingoweg 1**
**44139 Dortmund, DE y**
**EQ-3 AG (50.0%)**

(72) Inventor/es:

**DANKE, ENNO;**
**GROHMANN, BERND y**
**LUX, DANIEL**

(74) Agente/Representante:

**VALLEJO LÓPEZ, Juan Pedro**

## DESCRIPCIÓN

Procedimiento y dispositivo para controlar un sistema de automatización doméstica

El objeto se refiere a un procedimiento para operar un aparato de control central para un sistema de automatización doméstica. Además, el objeto se refiere a un procedimiento para integrar un aparato en un sistema de automatización doméstica. El objeto se refiere también a un aparato de control central para un sistema de automatización doméstica y a un aparato para un sistema de automatización doméstica.

Sistemas para la automatización doméstica son bien conocidos. Así, por ejemplo, bajo la denominación EIB/KNX es conocido un sistema de automatización doméstica alámbrico en el que se intercambian mensajes mediante un bus de serie entre sensores y actuadores y se controlan consumidores eléctricos de manera correspondiente a reglas previamente establecibles (parámetros). Sin embargo, un sistema de bus de este tipo requiere un cableado complicado que se puede realizar casi exclusivamente en una obra nueva.

Además es conocido también un sistema de automatización doméstica de radio por el documento US 2005/0120246 A1 cuya unidad de control puede controlar más de un aparato y es capaz de comunicarse de forma cifrada con éstos mediante las claves públicas existentes en los aparatos.

En el reequipamiento de soluciones de automatización doméstica en instalaciones eléctricas existentes son adecuadas en particular soluciones de radio de este tipo. A este respecto se comunican sensores y actuadores así como ordenadores de control centrales mediante radiodifusión de alta frecuencia. Sin embargo, dado que en el reequipamiento no existe una alimentación eléctrica en muchos puntos en los que se emplean sensores o actuadores, son necesarios al menos sensores autoalimentados con energía (por ejemplo, mediante baterías, condensadores, etc.). Sin embargo, en los sensores autoalimentados, el consumo eléctrico es un criterio decisivo para la duración de la operación del sensor con una única batería. Sensores que se comunican de forma ininterrumpida con actuadores y ordenadores de control centrales o se comunican en intervalos regulares con los actuadores o los ordenadores de control centrales consumen una cantidad innecesaria de corriente. Por tanto, ya es conocido prolongar la vida útil de la batería por que se trasladan los aparatos a un modo de espera y sólo en caso de una interacción de usuario en el aparato se trasladan a un modo activo y emiten y reciben mensajes.

La comunicación de los aparatos entre sí y entre los aparatos y el ordenador de control central se debe realizar preferiblemente de forma cifrada. Esto es válido en particular teniendo en cuenta que, en caso contrario, se podría influir mediante accesos por terceros en el control de un sistema de automatización doméstica. Así, por ejemplo, sería posible que se influya desde fuera en funciones de alarma. También sería posible influir en funciones eléctricas fuera de un edificio mediante un software y un hardware adecuados sin que el usuario lo desee. Por este motivo, una comunicación segura es un requisito casi obligatorio para un sistema de automatización doméstica seguro y que funciona.

Sin embargo, una comunicación segura es sólo posible cuando una clave de red, con la que se cifran mensajes, es conocida por todos los usuarios de comunicación y, dado el caso, sólo es válida para un sistema de automatización doméstica especial. Por tanto, es necesario que, en la integración de un aparato en una red, este aparato reciba la clave de red.

También puede ocurrir debido a una transmisión por radio que varias redes de radio se encuentren al alcance de un aparato nuevo. De este modo, las redes de radio pueden influir unas en otras cuando ninguna clave de red asegura la respectiva red de radio.

Adicionalmente, algunos aparatos se encuentran habitualmente en el modo de espera y sólo se activan cíclicamente de forma sincronizada en el caso de acciones de usuario o por una ráfaga de activación para ahorrar energía. A diferencia de los mecanismos establecidos tales como, por ejemplo, en el caso de WLAN, habitualmente, los aparatos no tienen una interfaz de usuario con la que se puede seleccionar la red deseada o se puede introducir una clave.

Por este motivo, el objeto se basó en el objetivo de proporcionar un sistema de automatización doméstica en el que se realice de manera fiable y de fácil manejo para el usuario un intercambio de claves. En particular debe ser posible un intercambio de claves sin entrada de usuario, en particular sin entrada de usuario en el aparato. Además, el intercambio de claves debe ser posible con aparatos que habitualmente se encuentran en el modo de espera y que por motivos de consumo energético no pueden estar activos permanentemente hasta el intercambio de claves.

Este objetivo se consigue de acuerdo con un aspecto mediante un procedimiento de acuerdo con la reivindicación 1.

Se ha reconocido que la seguridad necesaria para la distribución de una clave de red se puede garantizar cuando un aparato nuevo en una solicitud de integración de aparato ya envía una clave temporal que se utiliza por el aparato de control central para cifrar y distribuir la clave de red. Dado que la clave de red posibilita el descifrado de todo el tráfico de red, se debe evitar que aparatos no autorizados reciban esta clave. Por tanto, antes de que la clave de red

se transmita al aparato, por ejemplo, se puede solicitar una autorización por parte del usuario.

También es posible visualizar al menos la identificación de aparato en una pantalla tras la recepción. Mediante la identificación de aparato determinada en la etapa b) y, dado el caso, la visualización en la etapa c) de la identificación de aparato, es posible para el usuario autorizar un aparato. Esto se puede realizar, por ejemplo, mediante una interfaz de usuario gráfica de un aparato de mando. Por ejemplo, la interfaz puede ser una página HTML. También se pueden realizar aplicaciones en un ordenador personal o aparato móvil que posibilitan la autorización. Por ejemplo, una aplicación puede ser una aplicación Silverlight en un ordenador personal o aparato móvil (Smart Phone, Tablet PC, etc.). Asimismo, la autorización se puede realizar sin interacción de usuario. Entonces no es necesario visualizar la identificación. También se puede realizar una visualización de modo que sólo se visualiza que un aparato pretende integrarse sin visualizar la identificación de aparato. Por regla general, un usuario sabe cuando ha conectado aparatos nuevos y, por tanto, puede autorizar la integración de estos aparatos nuevos sin conocer obligatoriamente la identificación de aparato.

Por ejemplo, es posible que la identificación de aparato sea un número de serie. Mediante estas informaciones y mediante informaciones adicionales con respecto al aparato, por ejemplo, recibidas mediante Internet, que se pueden determinar mediante la identificación de aparato, el usuario puede realizar una autorización activa.

Después de que el aparato nuevo se haya autorizado en el aparato de control, el aparato de control envía una clave de red en la etapa d) en el marco de un mensaje KEY_OFFER. Con esta clave de red es posible el cifrado del tráfico de red. Sin embargo, la clave de red se cifra en la emisión con la clave temporal.

Con el procedimiento descrito se pueden registrar aparatos nuevos en el aparato de control central mediante una solicitud de integración de aparato (INCLUSION_REQ) y, en el caso de una autorización con éxito mediante un usuario, los aparatos nuevos reciben la clave de red en un mensaje KEY_OFFER.

Puede ocurrir que un aparato se traslade al modo de espera entre el mensaje a) y el mensaje d). En este caso, el aparato no recibe la clave de acuerdo con el mensaje d). Si se activa un aparato de este tipo mediante una interacción de usuario, por ejemplo, un acontecimiento, entonces envía de nuevo el mensaje de acuerdo con la etapa a). En este caso ya existe una autorización y se puede enviar la clave de acuerdo con la etapa d) directamente a continuación de la recepción de un mensaje de acuerdo con la etapa a) para asegurar que la clave se recibe por el aparato mientras que está activado. Es decir, un mensaje de acuerdo con la etapa d) se puede enviar directamente tras la recepción de una solicitud de integración de aparato (la siguiente) como reacción frente a la autorización de aparato.

Un aparato puede ser un sensor y/o un actuador.

Un sensor puede ser, por ejemplo, un interruptor, un detector de movimientos, un palpador, un contacto de puerta, un termostato, un contacto de ventana, un sensor de imágenes, un sensor de claridad, un sensor de temperatura, un sensor binario, un micrófono u otro dispositivo para detectar cambios medioambientales.

Un actuador puede ser en particular un relé, una válvula, un motor, un motor de ajuste, un amortiguador de la luz, un dispositivo de control de persiana, un interruptor, un emisor de señales, un emisor de señales infrarrojas, un emisor de señales acústicas, un elemento de mando, un terminal de información u otro aparato para realizar procesos de conmutación, procesos de control, procesos de regulación u otras acciones y/o para emitir informaciones y estados.

Un aparato de control central (servidor, Smart Home Controller SHC) puede ser un ordenador dispuesto de forma central que asume funciones de control. Sin embargo, el aparato de control central también puede ser cualquier otro aparato configurado para distribuir una clave de red. Así se pueden ejecutar las funciones de dicho aparato de control "central", por ejemplo, también por un encaminador, un mando a distancia, aparatos de mando o cualquier otro aparato (sensor, actuador) en el entorno de automatización. El aparato de control central (servidor) puede procesar y emitir parámetros para la configuración de sensores y actuadores. Asimismo, el servidor puede ser responsable de una gestión de claves de comunicación central. En particular, el servidor puede ser responsable de una notificación central de una clave de red. Por ejemplo, el servidor puede estar conectado con una red de área amplia. A este respecto, por ejemplo, es posible que el servidor esté conectado mediante un encaminador correspondiente con una red de área amplia, por ejemplo, una red de área amplia basada en TCP/IP. En particular puede ser posible acceder al servidor mediante la red de área amplia y realizar de forma remota configuraciones. El servidor puede ser tal que sólo se comunica con sensores y actuadores para fines de comunicación. Además, el sistema de automatización doméstica puede estar diseñado de modo que se realiza una comunicación entre sensores y actuadores para el control como reacción frente a acontecimientos sin que el servidor esté interconectado. De este modo se puede realizar una automatización doméstica autónoma que también funciona sin un servidor. Sin embargo, esto sólo es posible de manera segura cuando es conocida una clave de red para el cifrado de comunicación en los aparatos.

Con el procedimiento descrito es posible intercambiar de manera fiable claves de red. Básicamente, un intercambio de claves no es seguro de forma criptográfica, ya que para ello se tendrían que utilizar un procedimiento tal como

DIFFIE-HELL-MANN o certificados. Sin embargo, en el procedimiento descrito, un posible atacante tiene que grabar en el momento correcto la clave temporal de la solicitud de integración de aparato (INCLUSION_REQ), a continuación, tras la autorización (temporalmente aleatoria) del aparato nuevo, grabar y descifrar el mensaje KEY_OFFER para así obtener la clave de red. Estos dos momentos raros y aleatorios proporcionan una seguridad suficiente en el ámbito de aplicación privado.

Un aparato nuevo en el sentido de la reivindicación 1 puede ser tanto un aparato nuevo que se integra en la red de automatización doméstica como un aparato que se ha restablecido al estado de entrega. También es posible que un aparato nuevo sea un aparato que se ha excluido del sistema de automatización doméstica existente y se debe integrar de nuevo.

La determinación de al menos una identificación de aparato y de una clave temporal a partir de la solicitud de integración de aparato, por ejemplo, también puede significar que sólo la identificación de aparato se determina a partir de la solicitud de integración de aparato y, entonces, la clave temporal se genera en la centralita. En la siguiente etapa d), la clave de red se puede cifrar entonces con la clave temporal y, a continuación, la clave de red cifrada se puede transmitir junto con la clave temporal (en el texto claro) al aparato. En este caso, la clave de red se cifra y la clave temporal se transmite en el texto claro. Sin embargo, un atacante no puede escuchar y tomar simplemente la clave de red cifrada sin conocimiento del protocolo de transmisión sino que, por un lado, tiene que conocer el protocolo de transmisión y, por otro lado, grabar la clave temporal que se envía conjuntamente en la transmisión de la clave de red cifrada.

Para asegurar que la clave de red también se ha recibido en el aparato se propone de acuerdo con un ejemplo de realización ventajoso que la emisión de la clave de red cifrada (KEY_OFFER 64) se realice directamente tras la recepción de una solicitud de integración de aparato de acuerdo con la etapa a) como reacción frente a la autorización de aparato (62, 72) y/o que tras la emisión de la clave de red se vigile la recepción de un mensaje de acuse de recibo de clave (KEY_ACK). De este modo, el ordenador de control central puede vigilar si la clave de red realmente se ha recibido y descifrado en el aparato. El aparato responde con un mensaje KEY_ACK y, a continuación, forma parte de la red.

En la etapa b) se transmite al menos la identificación de aparato con ayuda de la solicitud de integración de aparato. Esta identificación de aparato se puede utilizar para la visualización y para la autorización.

En el marco de la autorización es posible que en el lado del ordenador de control se descifren una clave de red con la clave temporal que se ha generado en el aparato y se ha transmitido con la solicitud de integración de aparato o que se ha generado en el lado del ordenador de control, una vez que se haya realizado una autorización de aparato y se haya autorizado el aparato. La clave de red cifrada con la clave temporal se puede cifrar entonces adicionalmente con una clave de aparato almacenada permanentemente en el ordenador de control. La clave de aparato se puede determinar en el lado del ordenador de control mediante la identificación de aparato. La clave de aparato puede ser conocida tanto en el aparato como en el ordenador de control. A este respecto puede existir una asignación unívoca entre la identificación de aparato y la clave de aparato. Se puede realizar en el ordenador de control mediante la identificación de aparato un cifrado específico del aparato de la clave de red, en particular de la clave de red cifrada con la clave temporal. La clave de red cifrada así con la clave temporal y/o la clave de aparato se puede transmitir al aparato. Además, la clave temporal se puede transmitir al aparato.

En la comunicación entre el aparato y el ordenador de control se puede transmitir la clave temporal junto con la clave de red cifrada con la clave de aparato y la clave temporal en el texto claro al aparato. Incluso si se escuchara la clave temporal no se podría realizar un descifrado de la clave de red, ya que ésta está cifrada además con la clave de aparato.

En el aparato se descifra a continuación la clave de red cifrada con la clave de aparato y la clave temporal en primer lugar con la clave de aparato. La clave de aparato es conocida en el aparato y se puede utilizar para el descifrado, pero no se puede leer. A continuación, la clave de red cifrada ahora ya sólo con la clave temporal se puede descifrar con la clave temporal conocida en el aparato y la clave de red existe en el aparato para su uso adicional.

Para el descifrado de la clave de red o de la clave de red cifrada con la clave temporal es necesaria una clave de aparato individual. Por ejemplo, ésta puede existir en un servidor/servicio de clave de aparato. Así, por ejemplo, es posible que la clave de red cifrada con la clave temporal se transmita por el ordenador de control al servidor/servicio de clave de aparato. Además, la identificación de aparato se transmite por el ordenador de control al servidor/servicio de clave de aparato. En el servidor/servicio de clave de aparato se determina una clave de aparato con ayuda de la identificación de aparato. Con ayuda de la clave de aparato se descifra la clave de red cifrada con la clave temporal. La clave de red cifrada entonces con la clave de aparato y la clave temporal se transmite por el servidor/servicio de clave de aparato al ordenador de control y, desde allí, al aparato.

El servidor/servicio de clave de aparato puede ser un único servidor de clave. Asimismo, el servidor/servicio de clave de aparato puede estar formado a partir de una pluralidad de servidores. Por ejemplo, el ordenador de control puede haber almacenado en un fichero de configuración la dirección de al menos un servidor de clave. También es posible

que sea conocido un servidor de clave central en el ordenador de control central, aunque el servidor de clave central retransmite solicitudes de ordenadores de control centrales de forma dinámica a servidores de clave adicionales para de este modo conseguir un control de carga.

Un aparato de control adicional que, por ejemplo, también había recibido la solicitud de integración de aparato y había almacenado de forma intermedia la clave temporal y, a continuación, intentó incluir el aparato en la red propia mediante un mensaje KEY_OFFER, recibe del aparato, por ejemplo, un mensaje de rechazo de recepción de clave (KEY_NAK). Por tanto, el usuario del segundo aparato de control recibe, por ejemplo, mediante una visualización una información de que el aparato se ha incluido en otra red.

Sin embargo, si el usuario del segundo aparato de control está en posesión del aparato incluido en una red externa y si recibe un mensaje KEY_NAK, una vez que haya pretendido integrar el aparato, el propio usuario puede restablecer el aparato que se encuentra en su posesión al estado de entrega y, de este modo, eliminar la integración en la red externa y realizar un nuevo intento de integración.

De acuerdo con un ejemplo de realización ventajoso se propone que sólo tras la recepción del mensaje de acuse de recibo de clave se integra el aparato nuevo por el aparato de control en el sistema de automatización doméstica. Con ello se asegura que el aparato de control central vigila el intercambio correcto de la clave de red con el aparato nuevo y sólo en caso de un intercambio correcto integra el aparato en la red.

Para reducir el riesgo de que un aparato de control central no deseado reciba la solicitud de integración de aparato o, tal como se describe a continuación, un mensaje de búsqueda de integración (INCLUSION_DISCOVER), se propone de acuerdo con un ejemplo de realización ventajoso que el aparato de control central sólo se habilite para recibir y/o evaluar mensajes de este tipo de un aparato nuevo mediante una activación de un modo de integración. La activación de un modo de integración se puede realizar, por ejemplo, mediante interacciones de usuario, por ejemplo, mediante la apertura de un lado de integración en el aparato de control.

Por ejemplo, es posible que un modo de integración de este tipo permanezca activo durante un determinado intervalo de tiempo, por ejemplo, de 5 minutos, y, a continuación, se desactive automáticamente. Dentro de este intervalo de tiempo, el aparato de control central puede evaluar solicitudes de integración de aparato de los aparatos nuevos. Fuera de este intervalo de tiempo se pueden ignorar las solicitudes de integración de aparato. También es posible que se evalúen solicitudes de integración de aparato mediante el aparato de control central y, en particular, que se determine la identificación de aparato. Con ayuda de la identificación de aparato es posible determinar si un aparato ya estaba integrado en la red y, dado el caso, se ha restablecido a los ajustes de fábrica. En este caso ya se realizó previamente una autorización del aparato y el ordenador de control conoce esta autorización. Al usuario se le puede ofrecer entonces rechazar la autorización y eliminar el aparato del sistema de automatización doméstica, volver a integrar el aparato en el sistema de automatización doméstica y, a este respecto, transmitir de nuevo la clave de red (preferiblemente cifrada) o también integrar el aparato como un aparato nuevo en el sistema de automatización doméstica, pudiendo asignarse entonces al aparato otros parámetros y ajustes. También es posible que en el estado de entrega del sistema de automatización doméstica estén asociados entre sí el ordenador de control central y al menos un aparato. Es decir, en el ordenador de control central ya está almacenada la identificación de aparato del aparato asociado con este ordenador de control. En este caso se puede detectar mediante la identificación de aparato que el aparato pertenece al dispositivo de control central. Una integración se puede realizar entonces, por ejemplo, también fuera del modo de integración. También es posible que ya no sea necesaria una autorización, ya que el aparato ya está asignado por fábrica al ordenador de control central.

De acuerdo con un ejemplo de realización ventajoso se propone que antes de la etapa a) se reciba en una etapa a0) un mensaje de búsqueda de integración (INCLUSION_DISCOVER) del aparato nuevo. Mediante la etapa a0) se activa un procedimiento de dos niveles que en primer lugar exige que los aparatos nuevos se den a conocer frente a aparatos de control centrales mediante un mensaje de búsqueda de integración. El aparato envía un mensaje de búsqueda de integración (INCLUSION_DISCOVER) tras la activación de un modo de inclusión en el aparato para indicar que aún no tiene una clave de red y pretende ser incluido por un aparato de control en una red. Por tanto, preferiblemente, un mensaje de búsqueda de integración sólo se emite por un aparato nuevo si se ha trasladado a un modo de integración y aún no ha almacenado una clave de red.

Para posibilitar al aparato de control identificar el aparato nuevo que desea la integración en la red se propone de acuerdo con un ejemplo de realización ventajoso que junto con el mensaje de búsqueda de integración se transmita una identificación de aparato del aparato nuevo. Con ayuda de la identificación de aparato, por un lado, es posible identificar el aparato nuevo. Por otro lado, es posible responder de forma dirigida a este aparato mediante la identificación de aparato. Así se puede utilizar en la respuesta del aparato de control central la identificación de aparato para direccionar el aparato que ha emitido el mensaje de búsqueda de integración.

De acuerdo con un ejemplo de realización ventajoso se propone que tras la etapa a0) y antes de la etapa a) se emita en una etapa a1) un mensaje de oferta de integración (INCLUSION_OFFER) al aparato nuevo. Si un aparato de control se encuentra en el modo de integración y recibe un mensaje de búsqueda de integración, el aparato de control responde con un mensaje de oferta de integración (INCLUSION_OFFER). El mensaje de oferta de

integración está asignado preferiblemente mediante la identificación de aparato de forma unívoca a un aparato nuevo. Mediante el mensaje de oferta de integración, el aparato de control señala al aparato nuevo que está listo para emitir una clave de red. El aparato nuevo recibe mediante el mensaje de oferta de integración la información de que el aparato de control también se encuentra en el modo de integración y puede recibir una clave temporal. De este modo se asegura que las claves temporales sólo se emiten por aparatos nuevos cuando realmente existen aparatos de control que en el modo de integración pueden recibir la recepción de la clave temporal en el marco de una solicitud de integración de aparato (INCLUSION_REQ). De este modo se reduce el número de las veces con las que se emite la clave temporal.

De acuerdo con un ejemplo de realización ventajoso se propone que la clave recibida en la etapa b) esté formada a partir de al menos dos claves, siendo una primera clave una clave generada de forma temporal en el aparato que está cifrada con una clave almacenada permanentemente en el aparato. La clave temporal se puede almacenar de forma intermedia en uno o varios aparatos de control. Por ejemplo, la clave temporal se puede generar de nuevo tras cada restablecimiento del aparato al estado de entrega para también garantizar la seguridad en el caso de una retransmisión de aparatos. Sin embargo, para evitar que la clave temporal se escuche por una persona extraña, la clave temporal se puede cifrar con una clave almacenada de forma permanente en el aparato. Por ejemplo, una clave de este tipo almacenada de forma permanente en el aparato puede estar definida previamente en el proceso de producción. Siempre que una clave previamente definida de este tipo no se de a conocer sino sólo esté almacenada en los aparatos y en los aparatos de control centrales, el cifrado de la clave temporal es seguro, ya que ésta está cifrada con la clave almacenada de forma permanente.

También es posible que la clave temporal se intercambie en el texto claro entre el aparato y el aparato de control. Esto se puede realizar tanto en el marco de la solicitud de integración de aparato por el aparato al aparato de control como en la emisión de la clave de red cifrada como reacción frente a la autorización de aparato por el aparato de control al aparato.

Un intercambio de claves seguro es posible, por ejemplo, con ayuda del servidor de clave. A este respecto, la clave temporal puede ser conocida en el aparato de control y en el aparato y se puede transmitir en el trayecto entre el aparato de control y el aparato en el texto claro. La clave de aparato es conocida sólo por el aparato y el servidor de clave y no se transmite de forma no cifrada. Finalmente, la clave de red es conocida sólo en el aparato de control y se debe dar a conocer al aparato, pero no al servidor de servicio de clave. Para conseguir esto, la clave de red conocida en el aparato de control se cifra en primer lugar con la clave temporal. A continuación, la clave de red cifrada con la clave temporal se transmite al servidor de servicio de clave junto con la identificación de aparato. Dado que el servidor de servicio de clave no conoce la clave temporal, no puede descifrar la clave de red. El servidor de servicio de clave cifra con la clave de aparato la clave de red cifrada con la clave temporal. Esta clave de red cifrada así se transmite por el servidor de servicio de clave al aparato de control y, desde allí, se retransmite al aparato. En el trayecto de transmisión entre el aparato de control y el aparato, la clave temporal se podría haber escuchado. Sin embargo, dado que la clave de red en el trayecto entre el aparato de control y el aparato se ha cifrado adicionalmente con la clave de aparato, es imposible descifrar la clave de red también conociendo la clave temporal sin conocer la clave de aparato. Dado que la clave de aparato sólo es conocida en el aparato y en el servidor de servicio de clave, un atacante no puede escuchar la clave de red. En el aparato es conocida la clave temporal. Ésta se ha generado en el aparato o se ha transmitido en el marco del mensaje de acuerdo con la etapa d) en el texto claro. En el aparato se descifra entonces en primer lugar con la clave de aparato la clave de red cifrada con la clave temporal y la clave de aparato. A continuación, la clave temporal se utiliza para descifrar la clave de red que ya sólo está cifrada con la clave temporal. En el aparato existe entonces la clave de red que se puede utilizar para la comunicación adicional.

De acuerdo con un ejemplo de realización ventajoso se propone que la autorización de aparato se realice mediante una interacción de usuario o por que se consulta una asignación almacenada de forma central entre la identificación de aparato y el aparato de control y, en el caso de un resultado de consulta positivo, se realiza automáticamente una autorización. Por un lado, es posible que se pueda realizar la autorización de forma controlada por el usuario. Para ello se puede visualizar la identificación de aparato a un usuario en una pantalla y se puede invitar al usuario a autorizar el aparato correspondiente. Por otro lado, es también posible que se realice automáticamente una autorización. Así, por ejemplo, una asociación entre el aparato y el aparato de control ya se puede almacenar en un sistema logístico. Por ejemplo, el cliente puede asociar el aparato de control correspondiente con el aparato nuevo al comprar un aparato, por ejemplo, al indicar un número de aparato de control. Si se exige ahora una autorización, el aparato de control, por ejemplo, puede recurrir a asociaciones así almacenadas mediante Internet y puede comprobar que el aparato nuevo está asignado al aparato de control. Si éste es el caso, se puede realizar una autorización automáticamente, es decir, sin una interacción de usuario.

De acuerdo con un ejemplo de realización ventajoso se propone que el mensaje de oferta de integración emitido en la etapa a1) incluya una identificación de aparato de control y que la solicitud de integración de aparato recibida en la etapa a) incluya la identificación de aparato de control. Con la identificación de aparato de control es posible para el aparato direccionar la solicitud de integración de aparato al aparato de control.

De acuerdo con un ejemplo de realización ventajoso se propone que se active un modo de integración del aparato de control mediante una interacción de usuario y que sólo en el modo de integración se puedan recibir y/o evaluar mensajes de acuerdo con la etapa a0) y/o a) y/o que el modo de integración se desactive tras un tiempo definido tras la interacción de usuario. Tal como ya se describió anteriormente, mediante la activación de un modo de integración mediante una interacción de usuario se evita que aparatos de control se encuentren en todo momento en el modo de integración y, por tanto, se produzcan permanentemente situaciones de competencia entre dos aparatos de control que en realidad están asignados a dos redes independientes.

De este modo, por ejemplo, a mensajes INCLUSION_DISCOVER de aparatos de control sólo se responde si están integrados en el modo de integración, a mensajes INCLUSION REQ, por ejemplo, sólo se responde si el mensaje INCLUSION REQ se ha recibido y evaluado en el modo de integración y/o si ya ha tenido lugar previamente la autorización del aparato, lo que evita el riesgo de que se comuniquen claves de red falsas a aparatos nuevos.

Un aspecto adicional es un procedimiento de acuerdo con la reivindicación 10.

Mediante este procedimiento es posible en el aparato nuevo solicitar una integración en una red por un aparato de control central y recibir de manera segura una clave de red por el aparato de control central.

De acuerdo con un ejemplo de realización ventajoso se propone que antes de la etapa b) se emita en una etapa b0) un mensaje de búsqueda de integración. Con ayuda del mensaje de búsqueda de integración, el aparato nuevo señala frente a un aparato de control que desea integrarse en la red. Este mensaje de búsqueda de integración se emite preferiblemente en el modo de difusión de modo que todos los aparatos de control que se encuentran al alcance de comunicación reciben este mensaje.

Para asegurar que el mayor número posible de aparatos de control al alcance de comunicación reciban un mensaje de búsqueda de integración de este tipo se propone que la etapa b0) se repita tras el acontecimiento en un número previamente establecible. "Reintentos" de este tipo aumentan la perceptibilidad del mensaje y la posibilidad de que aparatos de control reciban este mensaje. También se pueden realizar las etapas de acuerdo con a) en un número o tiempo previamente establecido.

Para evitar que se realice una integración por un aparato de control en cualquier momento, una vez que se emita un mensaje de búsqueda de integración, se propone de acuerdo con un ejemplo de realización ventajoso que de acuerdo con la etapa b0) se vigile en un tiempo previamente establecible la recepción de un mensaje de oferta de integración. Con ello se espera a un mensaje de oferta de integración en un tiempo determinado después de que se emita un mensaje de búsqueda de integración.

De acuerdo con un ejemplo de realización ventajoso se propone que, en el caso de que no se produzca el mensaje de oferta de integración o un mensaje de integración de aparato, el aparato se desactive (se traslade al modo de espera). Esto ahorra corriente, ya que, de este modo, el aparato sólo tiene que esperar un tiempo determinado tras la interacción de usuario a una respuesta de un aparato de control central.

De acuerdo con un ejemplo de realización ventajoso se propone que de acuerdo con la etapa b0) en una recepción de un mensaje de oferta de integración se envíe la solicitud de integración de aparato. Esto asegura que la clave temporal también se envía sólo cuando al menos un aparato de control espera posiblemente la recepción de una solicitud de integración de aparato. Si el aparato dispone de una interfaz de usuario gráfica, se puede enviar también de forma controlada por el usuario una solicitud de integración de aparato a un aparato de control que se puede seleccionar. De este modo, el usuario puede seleccionar con qué aparato de control se debe conectar el aparato.

De acuerdo con un ejemplo de realización ventajoso se propone también que el acontecimiento que activa el modo de integración sea una interacción de usuario, un encendido del aparato o un restablecimiento del aparato al estado de entrega, activándose, por ejemplo, el modo de integración exclusivamente para el caso de que aún no se haya recibido una clave de red en el aparato.

De acuerdo con un ejemplo de realización ventajoso se propone que la clave de red se reciba junto con una identificación de aparato de control. De este modo es posible en el aparato nuevo asignar la clave de red a un aparato de control y acusar el recibo de la clave de red al aparato de control.

Por este motivo se propone de acuerdo con un ejemplo de realización ventajoso que la clave de red recibida se confirme con respecto al aparato de control con un mensaje de acuse de recibo de clave (KEY_ACK) mediante el uso de la identificación de aparato de control. Con ayuda de este mensaje, el aparato de control puede asegurar que la clave de red se ha recibido correctamente en el aparato nuevo.

De acuerdo con un ejemplo de realización ventajoso se propone que para el caso de que ya se haya recibido previamente otra clave de red se emita un mensaje de rechazo de recepción de clave (KEY_NAK). Con ayuda de este mensaje, el aparato de control central puede determinar que el aparato nuevo ya se ha integrado por otro aparato de control. Para el usuario resulta de ello la ventaja de que puede controlar si se ha integrado un aparato

que es suyo por otro aparato de control. En un caso de este tipo, puede restablecer el aparato para iniciar un nuevo intento de integración con el aparato de control propio.

Un aspecto adicional es un aparato de control central para un sistema de automatización doméstica de acuerdo con la reivindicación 14.

Un aspecto adicional es un aparato para un sistema de automatización doméstica de acuerdo con la reivindicación 15.

En la entrada del aparato se puede detectar un acontecimiento de acuerdo con el objeto. Un acontecimiento puede ser una interacción de usuario, por ejemplo, el accionamiento de un interruptor o palpador, un cambio de condiciones medioambientales, un movimiento, una apertura de una ventana, un cambio de temperatura u otro cambio de condiciones ambientales.

En la detección de un acontecimiento, el aparato, preferiblemente un aparato autoalimentado (operado por acumulador), se puede activar y se puede trasladar a un modo activo. De acuerdo con el objeto es posible que el aparato en el estado normal se encuentre en un estado de reposo (modo de espera). En este estado de reposo sólo se vigila la entrada con respecto a la ocurrencia de un acontecimiento. Todas las demás funciones se pueden desactivar o se pueden mantener con una absorción de potencia mínima. En particular, la comunicación mediante una interfaz de comunicación puede estar suspendida en estos periodos de tiempo, de modo que ni se emiten señales ni se reciben señales. En la detección de un acontecimiento, el aparato se puede activar (cambiar al modo activo) de modo que el procesador se activa y se activa la interfaz de comunicación para la comunicación con el entorno.

Por ejemplo, el procesador puede ser un procesador digital de señales (DSP). Asimismo, el procesador puede ser un microcontrolador. El procesador puede ser cualquier microprocesador que está configurado, por un lado, para evaluar señales de entrada y, por otro lado, para emitir señales de control.

Por ejemplo, la interfaz de comunicación en un aparato o en el aparato de control puede ser un dispositivo para la comunicación mediante una red inalámbrica. Asimismo, la interfaz de comunicación se puede comunicar mediante una red inalámbrica. Por ejemplo, se puede realizar una comunicación mediante LAN, WLAN, Bluetooth o similares. En particular, por ejemplo, la interfaz de comunicación puede emitir mensajes con una frecuencia de 868 Mz con una clave de desplazamiento de frecuencia. En particular son posibles tasas de transmisión de datos de 10 KB/s. Un protocolo de acceso puede ser, por ejemplo, un protocolo de acceso CSMA/CA.

La comunicación mediante la interfaz de comunicación puede ser una comunicación bidireccional en un bus, en particular en un bus de radio. La interfaz de comunicación puede estar configurada para cifrar los datos transmitidos. En particular, un cifrado simétrico puede estar asistido por la interfaz de comunicación. En particular, un cifrado CCM o un cifrado CCM* puede estar asistido. En particular se puede utilizar un procedimiento de cifrado autenticado de acuerdo con la norma IEEE 802.11. También es posible un procedimiento de cifrado ampliado de acuerdo con el modo de contador estándar de cifrado avanzado (AES/CCM) en el que se utiliza una cifra de bloque de 16 bytes. Para el cifrado simétrico puede ser posible que cada sensor, cada actuador y cada ordenador de control central (servidor) tenga un número de serie. También puede ser posible que el número de serie de cada aparato sea conocido en una centralita. La comunicación mediante la interfaz de comunicación se puede realizar tanto en multidifusión como en unidifusión.

Los procedimientos anteriormente mencionados se pueden realizar también como programa informático o como programa informático almacenado en un medio de almacenamiento. A este respecto puede estar programado de manera adecuada mediante un programa informático en el lado del sensor, en el lado del actuador y/o en el lado del servidor un microprocesador para realizar las respectivas etapas de procedimiento. Las características de los procedimientos y dispositivos se pueden combinar libremente entre sí. En particular, características de las reivindicaciones dependientes omitiendo las características de las reivindicaciones independientes pueden ser inventivas por sí solas o de forma libremente combinada entre sí independientemente.

A continuación se explica en más detalle el objeto mediante un dibujo que muestra ejemplos de realización.

La figura 1 muestra de manera esquemática un aparato que está formado como sensor;

La figura 2 muestra de manera esquemática un aparato que está formado como actuador;

La figura 3 muestra una estructura esquemática de un sistema de automatización doméstica;

La figura 4 muestra el desarrollo de un procedimiento de acuerdo con un ejemplo de realización;

La figura 5 muestra el desarrollo de un procedimiento de acuerdo con un ejemplo de realización ejemplar adicional;

La figura 6 muestra el desarrollo de un procedimiento de acuerdo con un ejemplo de realización ejemplar adicional;

La figura 7 muestra el desarrollo de un procedimiento de acuerdo con un ejemplo de realización ejemplar adicional;

La figura 8 muestra el desarrollo de un procedimiento de acuerdo con un ejemplo de realización ejemplar adicional;

La figura 9 muestra el desarrollo de un procedimiento de acuerdo con un ejemplo de realización ejemplar adicional;

La figura 10 muestra el desarrollo de un procedimiento de acuerdo con un ejemplo de realización ejemplar adicional;

La figura 11 muestra el desarrollo de un procedimiento de acuerdo con un ejemplo de realización ejemplar adicional;

La figura 12 muestra el desarrollo de un procedimiento de acuerdo con un ejemplo de realización ejemplar adicional.

La figura 1 muestra de manera esquemática un sensor 2 con un campo de palpadores 4 que se utiliza como entrada para la detección de acontecimientos. En el sensor 2 está dispuesto además un procesador 6 para evaluar los acontecimientos detectados en el campo de palpadores 4. En el sensor 2 está prevista también una interfaz de radio 8 que se activa mediante el procesador 6. Mediante la interfaz de radio 8 es posible emitir y recibir mensajes mediante un protocolo de radio. La interfaz de radio 8 posibilita una comunicación mediante una interfaz aérea. Además está dispuesta en el sensor 2 una memoria 10. En la memoria 10 se pueden almacenar claves temporales y claves de red. Con ayuda del sensor 2 es posible registrar acontecimientos y convertirlos en mensajes correspondientes.

La figura 2 muestra un actuador 12. El actuador 12 tiene una salida 14 a través de la que, por ejemplo, se pueden controlar consumidores eléctricos. Se puede apreciar que, en el ejemplo representado, la salida 14 está conectada con un interruptor a través del que se pueden cortocircuitear o desconectar contactos eléctricos en la salida 14. La salida 14 o el interruptor se activa mediante un procesador 16 que también está dispuesto en el actuador 12. El procesador 16 está conectado con una interfaz de radio 18. Mediante la interfaz de radio 18 se pueden intercambiar datos mediante la interfaz aérea, por ejemplo, con la interfaz de radio 8 y con un servidor central.

Finalmente está dispuesta en el actuador 12 una memoria 20 en la que pueden estar almacenadas claves temporales y claves de red.

Los sensores 2 y los actuadores 12 mostrados en las figuras 1 y 2 se pueden emplear en un sistema de automatización doméstica mostrado en la figura 3. La figura 3 muestra, por ejemplo, el entorno 26 de una casa o de un piso. En este entorno 26 está previsto un encaminador 24 que proporciona una conexión de comunicación con Internet 28 y puede emitir paquetes de datos a Internet 28 y recibir éstos de Internet 28. Al encaminador 24 está conectado un servidor 22 (Smart Home Controller, SHC). Mediante el encaminador 24, el SHC 22 puede intercambiar paquetes de datos con Internet 28. El SHC 22 puede establecer una comunicación con los sensores 2 y con los actuadores 12 mediante una conexión de radio. La comunicación puede ser bidireccional y se puede realizar como respuesta a solicitudes.

A Internet 28 está conectada una unidad de gestión 30 central. La unidad de gestión 30 central puede iniciar una conexión con el SHC 22 mediante Internet 28 y el encaminador 24, por ejemplo, para realizar una configuración de los sensores 2, de los actuadores 12 o del SHC 22.

La configuración del SHC 22 y de los sensores 2 y de los actuadores 12 mediante Internet 28 se puede realizar, por ejemplo, por un ordenador personal 32a privado. Para ello, el ordenador personal 32a, por ejemplo, puede establecer una conexión mediante Internet 28 con la unidad de gestión 30 central y realizar una configuración del SHC 22, del sensor 2 o del actuador 12 mediante la unidad de gestión 30 central. Este cambio de configuración se puede transmitir entonces mediante Internet 28 por la unidad de gestión 30 central mediante el encaminador 24 al SHC 22. También se puede realizar una configuración, por ejemplo, mediante un teléfono móvil 32b, en la que el teléfono móvil 32b está conectado mediante una pasarela 34 con Internet 28 y puede iniciar una conexión con la unidad de gestión 30 central mediante la pasarela 34.

Una comunicación segura entre el SHC 22 y la unidad de gestión 30 central puede estar garantizada, por ejemplo, por que el SHC 22 establece un túnel de comunicación a través de Internet 28 con la unidad de gestión 30 central mediante el encaminador 24, una vez que el SHC 22 se conecte con el encaminador 24. Para ello, el SHC 22 sólo debe conocer la dirección IP fija de la unidad de gestión 30 central y cifrar mediante una contraseña y una clave la

comunicación con la unidad de gestión 30 central. Mediante esta conexión cifrada se puede realizar ahora una configuración del SHC 22, del sensor 2 y del actuador 12 por la unidad de gestión 30 central. La configuración se puede controlar por el ordenador personal 32a o por el teléfono móvil 32b. También es posible generar acontecimientos en el sensor 2 mediante el ordenador personal 32a y el teléfono móvil 32b para de este modo desencadenar determinadas acciones de los actuadores 12. También se puede consultar así el estado de los sensores 2 y de los actuadores 12.

La comunicación entre el SHC 22, los actuadores 12 y los sensores 2 posibilita, por un lado, la configuración de los sensores 2 y de los actuadores 12 y el control de consumidores eléctricos conectados al actuador 12 mediante los sensores 2. El control de actuador se regula mediante asociaciones entre un sensor 2 y actuadores 12 y también mediante parámetros de sensor y/o parámetros de actuador.

A los diferentes actuadores 12 se pueden conectar los consumidores eléctricos más diferentes. En la configuración del sensor 2 y de los actuadores 12 mediante el SHC 22 se puede reducir de acuerdo con el objeto el volumen de comunicación con un sensor 2, de modo que el sensor 2 autoalimentado con energía consume la menor cantidad posible de energía. Por ejemplo, los actuadores 12 se pueden alimentar permanentemente con energía, por ejemplo, pueden estar conectados a una alimentación de corriente y, de este modo, pueden recibir y emitir permanentemente mensajes. Asimismo, los actuadores 12 pueden estar configurados de modo que reciben permanentemente mensajes y emiten en intervalos mensajes. Asimismo, los actuadores 12 pueden estar configurados de modo que pueden recibir permanentemente mensajes y sólo emiten mensajes cuando sea necesario. El ahorro energético se debe realizar principalmente en los sensores 2 que están autoalimentados con energía.

La figura 4 muestra a modo de ejemplo los aparatos 2a-2e, 22 dispuestos en un entorno 26 de una casa. En la figura 4 se representa un usuario 34. Además se representa un servidor (ordenador de control central) 22 y un sensor 2a. Además se representan sensores adicionales 2b, 2c, 2d y 2e. Los sensores 2a-e podrían ser también actuadores. El sensor 2a es un sensor 2a que se activa mediante una interacción de usuario. El sensor 2b es un sensor 2b que se activa de forma sincronizada. El sensor 2c es un sensor 2c que se activa cíclicamente. El sensor 2d es un sensor 2d que se activa mediante una ráfaga de activación y el sensor 2e es un sensor 2e que está activado permanentemente. La comunicación mostrada a continuación está descrita sólo de forma ejemplar para los sensores 2a y 2e, aunque se puede transferir de forma análoga también a los sensores 2b-2d.

Además se representa en la figura 4 un servidor 42 dispuesto fuera del entorno 26 y un segundo usuario 44.

En la figura 4 y también en las siguientes figuras se representan los mismos aparatos con los mismos números de referencia. Además, las figuras 4 a 12 muestran los diagramas de mensajes en un flujo de mensajes entre los aparatos que tiene lugar mediante la interfaz de comunicación, preferiblemente, mediante una interfaz aérea.

Líneas continuas significan que los aparatos están activos. Líneas discontinuas significan que los aparatos están inactivos.

La figura 4 muestra un diagrama de mensajes en el que se integra un aparato que sólo se activa mediante una interacción de usuario en la red. Se puede observar que el usuario 34 active en primer lugar el sensor 2a 50. Tras una activación 50 del sensor 2a, el sensor 2a emite mensajes INCLUSION_DISCOVER 52 en el modo de difusión. Es decir, el mensaje INCLUSION_DISCOVER 52 no se direcciona a ningún receptor determinado. El mensaje INCLUSION_DISCOVER 52 se puede recibir tanto en el primer aparato de control 22 como en el segundo aparato de control 44. En la primera emisión del mensaje INCLUSION_DISCOVER 52, ni el primer aparato de control 22 ni el segundo aparato de control 42 se encuentra en un modo de integración, por lo que los aparatos de control 22, 42 no envían respuestas. Por tanto, el mensaje INCLUSION_DISCOVER 52 se emite de forma sucesiva un determinado número de veces, en el ejemplo mostrado dos veces, después de lo cual el sensor 2a se vuelve a trasladar al modo de espera.

A continuación, tal como se muestra en la figura 4, el primer aparato de control 22 se lleva al modo de integración 54. A continuación, el usuario 34 activa 50 el sensor 2a. A continuación, el sensor 2a envía de nuevo un mensaje INCLUSION_DISCOVER 52. El aparato de control 22 recibe el mensaje INCLUSION_DISCOVER 52 y, dado que se encuentra en el modo de integración, el aparato de control 22 responde al mensaje INCLUSION_DISCOVER 52 con un mensaje INCLUSION_OFFER 54. En el mensaje INCLUSION_OFFER 54 está incluida la identificación del aparato de control 22.

En cambio, el aparato de control 42 no se encuentra en el modo de integración, por lo que no se envía por el aparato de control 42 una respuesta al mensaje INCLUSION_DISCOVER 52.

Tras la recepción del mensaje INCLUSION_OFFER 56, el sensor 2a responde con un mensaje INCLUSION_REQ 58. En el mensaje INCLUSION_REQ 58 está incluida, por un lado, la identificación de aparato del sensor 2a y, por otro lado, una clave temporal.

La clave temporal se puede generar en la primera puesta en funcionamiento del sensor 2a. También es posible que la clave temporal se genere de nuevo para cada mensaje INCLUSION_REQ 58. También es posible que la clave temporal se cifre con una clave almacenada fijamente en el sensor 2a que también es conocida en el aparato de control 22.

También es posible que la clave temporal sólo se genere en el aparato de control y no en el sensor 2a.

El aparato de control 22 recibe el mensaje INCLUSION_REQ 58 y visualiza al usuario 34 mediante la identificación de aparato incluida en el mensaje INCLUSION_REQ 58 en una pantalla la identificación del sensor 2a 60.

En el ejemplo mostrado, el usuario 34 no reacciona frente a la visualización 60.

Dado que el sensor 2a aún no está integrado en una red, emite de nuevo un mensaje INCLUSION_DISCOVER 52.

Tras un tiempo indeterminado, el usuario 34 autoriza 62 al sensor 2a. Tras la autorización 62, el aparato de control 22 envía un mensaje KEY_OFFER 64 en el que está incluida una clave de red cifrada con la clave temporal. Junto con la clave de red cifrada se puede enviar la clave temporal (en caso de que éste se haya generado en el aparato de control 22) en el texto claro. Tal como se puede apreciar en la figura 4, el sensor 2a se encuentra en este momento en el modo de espera y no puede recibir el mensaje KEY_OFFER 64. El aparato de control 22 espera a un mensaje KEY_ACK 68, aunque no recibe a éste, ya que el sensor 2a se encuentra en el modo de espera y no emite un mensaje de este tipo.

En una interacción de usuario 66 nueva al sensor 2a, éste se activa. En este momento, el sensor 2a aún no ha recibido una clave de red y, a continuación, emite de nuevo un mensaje INCLUSION_DISOVER 52. El mensaje INCLUSION_DISCOVER 52 se recibe en el aparato de control 22 y, mediante la identificación de aparato incluida en el mensaje INCLUSION_DISCOVER 52, el aparato de control 22 puede determinar que el usuario 34 ya ha autorizado a este sensor 2a en la etapa 62. Por este motivo, el aparato de control 22 envía de nuevo un mensaje KEY_OFFER 64 al sensor 2a. El sensor 2a acusa recibo del mensaje KEY_OFFER 64 con un mensaje KEY_ACK 68.

A continuación, el sensor 2a ha recibido la clave de red y el aparato de control 22 sabe que el sensor 2a tiene esta clave de red, con lo que el sensor 2a está integrado en la red.

Tal como se puede apreciar en la figura 4, el aparato de control 42 no responde a ningún mensaje INCLUSION_DISCOVER 52, de modo que el aparato de control 42 no integra el sensor 2a.

La figura 5 muestra el desarrollo de una integración de un aparato, siendo el aparato en la figura 5, que se debe integrar, el sensor 2e que está permanentemente listo para recibir. La figura 5 muestra que el modo de integración del aparato de control 22 se activa mediante el usuario 34 54. A continuación, el modo de integración se activa en el sensor 2e 50. Por tanto, tanto el aparato de control 22 como el sensor 2e se encuentra en el modo de integración. El desarrollo de las siguientes etapas se corresponde aproximadamente con el desarrollo descrito en la figura 4.

A un mensaje INCLUSION_DISCOVER 52 responde el aparato de control 22 que se encuentra en el modo de integración con un mensaje INCLUSION_OFFER 56 que se responde por el sensor 2e mediante un mensaje INCLUSION_REQ 58.

El sensor 2e se visualiza al usuario 60. Siempre que el usuario no autorice al aparato, no se realiza una transmisión de un mensaje KEY_OFFER 64. Es decir, el sensor 2e emite tras un determinado tiempo de nuevo un mensaje INCLUSION_DISCOVER 52. Tras un determinado tiempo puede occurir que el sensor 2e abandone el modo de integración. A continuación, el modo de integración se debe activar de nuevo 50, después de lo cual el sensor 2e emite de nuevo mensajes INCLUSION_DISCOVER 52.

Sólo en la autorización 62 del sensor 2e mediante el usuario 34 en el aparato de control 22, el aparato de control 22 transmite un mensaje KEY_OFFER 64 al sensor 2e que acusa recibo con un mensaje KEY_ACK 68. A continuación, el sensor 2e está integrado en la red del aparato de control 22.

La figura 6 muestra el desarrollo de un procedimiento en el que tanto el aparato de control 22 como el aparato de control 42 se encuentra en el modo de integración. Las etapas 50, 52 se corresponden con aquéllas de acuerdo con la figura 4. A diferencia de la figura 4, el usuario 34 activa 54a el modo de integración en el aparato de control 22 y el usuario 44 activa 54b el modo de integración en el aparato de control 42.

Tal como se puede apreciar, tanto el aparato de control 22 como el aparato de control 42 envía tras la recepción del mensaje INCLUSION_DISCOVER 52 en cada caso un mensaje INCLUSION_OFFER 56a y 56b. El sensor 2a recibe el mensaje INCLUSION_OFFER 56a del aparato de control 22 y envía al aparato de control 22 un mensaje INCLUSION_REQ 58a con la clave temporal. El sensor 2a recibe también el mensaje INCLUSION_OFFER 56b del aparato de control 42 y envía al aparato de control 42 un mensaje INCLUSION_REQ 58b también con la clave

temporal.

Tanto el aparato de control 22 como el aparato de control 42 visualiza al usuario el sensor 2a 60a, 60b. Siempre que no se haya recibido un KEY_OFFER en el sensor 2a, el sensor 2a envía de nuevo mensajes INCLUSION_DISCOVER 52.

En la figura 6 se muestra que el usuario 34 autoriza 62 al sensor 2a. Las siguientes etapas se corresponden con aquéllas en la figura 4. En la figura 6 se autoriza al sensor 2a sólo en el aparato de control 22 y no en el aparato de control 42, por lo que el sensor 2a se integra en la red del aparato de control 22.

La figura 7 muestra el desarrollo de un procedimiento de manera correspondiente a la figura 6. A diferencia de la figura 6, el sensor 2a no se autoriza 70 de forma activa tras la visualización 60b del sensor 2a en el aparato de control 42. Por tanto, el aparato de control 42 tampoco envía un mensaje KEY_OFFER al sensor 2a. Todas las demás etapas se corresponden con aquéllas en la figura 6, estando activado el modo de integración del aparato de control 22 54a antes de que haya tenido lugar una activación 54b del aparato de control 42, por lo que el aparato de control 22 ya emite un mensaje INCLUSION_OFFER 56 al sensor 2a antes de que se haya emitido un mensaje INCLUSION_OFFER 56b por el aparato de control 42.

La figura 8 muestra el desarrollo de un procedimiento tal como se representa en la figura 7, aunque, en la figura 8, este aparato también se autoriza 72 mediante el usuario 44 tras la visualización 60b del aparato en el aparato de control 42. De este modo, el aparato de control 42 envía también un mensaje KEY_OFFER 64b al sensor 2a. Tras la autorización 62 del sensor 2a en el aparato de control 22, éste también envía un mensaje KEY_OFFER 64a. Ambos mensajes KEY_OFFER 64a, 64b se emiten durante un modo de espera del sensor 2a, de modo que el sensor 2a no puede recibir ninguno de los dos mensajes KEY_OFFER 64a, 64b.

Tras una nueva activación 50 del sensor 2a, éste emite de nuevo mensajes INCLUSION_DISCOVER 52. Ambos aparatos de control 22, 42 reciben este mensaje INCLUSION_DISCOVER 52. En ambos aparatos de control se autorizó al aparato 62, 72. En el ejemplo mostrado, el aparato de control 42 transmite en primer lugar el mensaje KEY_OFFER 64b. El sensor 2a recibe temporalmente después el mensaje KEY_OFFER 64a del aparato de control 22. Dado que el mensaje KEY_OFFER 64b se recibió en primer lugar, el sensor 2a envía un mensaje KEY_ACK 68 al aparato de control 42 y un mensaje KEY_NAK 78 al aparato de control 22. De este modo, en el ejemplo mostrado en la figura 8, el sensor 2a se integra en la red del aparato de control 42 y no en la red del aparato de control 22.

El usuario del aparato de control 22 experimenta la integración defectuosa mediante el mensaje KEY_NAK 78. Si la integración en la red del aparato de control 42 es defectuosa y el usuario 34 está en posesión del sensor 2a, puede restablecer el sensor 2a e iniciar una nueva integración. De este modo se asegura que ningún aparato de control 42 externo puede integrar permanentemente el sensor 2a cuando el sensor 2a no está en posesión del usuario 44 del aparato de control 42 externo.

La figura 9 muestra el desarrollo de un procedimiento simplificado en el que se renuncia a los mensajes INCLUSION_DISCOVER 52 y los mensajes INCLUSION_OFFER 56 y el sensor 2a emite directamente tras la activación 50 del modo de integración un mensaje INCLUSION_REQ 58. Este mensaje INCLUSION_REQ 58 se emite a este respecto en el modo de difusión y ya no está dirigido a un aparato de control 22, 42 especial. Una vez que se haya activado el modo de integración en el aparato de control 42 54 y el sensor 2a también esté activado 50, se visualiza el sensor 2a al usuario 60 tras la recepción de un mensaje INCLUSION_REQ 58 en el aparato de control 22. La integración del sensor 2a en la red del aparato de control 22 se corresponde con la mostrada anteriormente con las etapas 62 a 68, emitiéndose, en lugar de un mensaje INCLUSION_DISCOVER 52, un mensaje INCLUSION_REQ 58, siempre que en el sensor 2a no esté almacenada una clave de red. Una vez que se haya realizado una autorización mediante el usuario, se transmite un mensaje KEY_OFFER 64b del aparato de control al sensor. En el mensaje KEY_OFFER está incluida de forma cifrada la clave de red. El cifrado de la clave de red se puede realizar de la siguiente manera.

Una clave temporal se puede generar en el aparato de control 42. La clave de red se cifra en primer lugar con la clave temporal. Además, mediante la identificación de aparato se determina una clave de aparato. Esta clave de aparato puede existir en el aparato de control 42. La clave de red cifrada con la clave temporal se cifra con la clave de aparato. En el mensaje KEY_OFFER se transmite la clave de red cifrada de este modo al sensor 2a. De manera paralela a ello se transmite en el texto claro la clave temporal. En el sensor 2a es posible con la clave temporal recibida un descifrado de la clave de red cifrada con la clave temporal y la clave de aparato. Entonces se realiza un descifrado de la clave de red cifrada ahora ya sólo con la clave de aparato con ayuda de la clave de aparato conocida sólo en el aparato.

Un aseguramiento adicional de la clave de red se puede realizar, por ejemplo, al generarse una clave temporal en el aparato de control 42 tras la autorización. La clave de red se cifra en primer lugar con la clave temporal. La clave de red cifrada se transmite junto con la identificación de aparato a un servidor de clave que, por ejemplo, es accesible mediante Internet. En el servidor de clave se determina mediante la identificación de aparato una clave de aparato y se cifra con ayuda de la clave de aparato la clave de red cifrada con la clave temporal. La clave de red cifrada con la

clave de aparato y la clave temporal, a su vez, se transmite mediante Internet al aparato de control 42. El aparato de control 42 transmite la clave de red cifrada de forma doble al sensor 2a y en el texto claro la clave temporal. Si se escucha la clave temporal, no es posible descifrar la clave de red, ya que ésta se ha cifrado adicionalmente con la clave de aparato. En el sensor 2a se descifra en primer lugar con ayuda de la clave de aparato la clave de red cifrada con la clave de aparato y la clave temporal. La clave de red cifrada entonces ya sólo con la clave temporal se descifra con la clave temporal enviada al aparato y en el aparato existe la clave de red.

La figura 10 muestra un ejemplo de realización en el que el sensor 2e se integra como aparato que permanentemente está listo para recibir. El procedimiento descrito en la figura 10 se diferencia del procedimiento descrito en la figura 9 sólo en que el mensaje KEY_OFFER 64 se recibe inmediatamente tras la autorización 62 del aparato en el sensor 2e y se realiza una confirmación.

El procedimiento mostrado en la figura 11 se corresponde con el procedimiento descrito en la figura 10, estando activados en el procedimiento descrito en la figura 11 tanto el aparato de control 22 como el aparato de control 42 54a, 54b y encontrándose éstos en el modo de integración. De este modo, el sensor 2e se visualiza en ambos aparatos de control 60a, 60b. Sin embargo, la autorización 62 se realiza sólo en el aparato de control 22, de modo que el sensor 2a sólo se integra mediante el aparato de control 22.

La visualización 60b del aparato nuevo frente al usuario 44 se puede ignorar o, asimismo, es posible que no se autorice al sensor 2a actuando de forma activa. En ambos casos, el sensor 2a se integra mediante el aparato de control 22 y no mediante el aparato de control 42.

La figura 12 muestra fundamentalmente un procedimiento ya descrito en la figura 8, emitiéndose en este caso, en lugar de los mensajes INCLUSION_DISCOVER 52 directamente mensajes INCLUSION_REQ 58. En la figura 12 se puede apreciar que, también en este caso, el aparato de control 42, cuyo mensaje KEY_OFFER 64 se recibió en primer lugar por el sensor 2a, integra el sensor 2a en su red.

**REIVINDICACIONES**

1. Procedimiento para operar un aparato de control central para un sistema de automatización doméstica con las etapas de

a) recibir una solicitud de integración de aparato (INCLUSION_REQ 58) de un aparato nuevo (2),
b) determinar al menos una identificación de aparato a partir de la solicitud de integración de aparato (INCLUSION_REQ 58),
c) evaluar una autorización de aparato (62, 72),
c1) cifrar una clave de red conocida en el aparato de control con una clave temporal,
c2) enviar la clave de red cifrada con la clave temporal junto con la identificación de aparato a un servidor de servicio de clave,
c3) recibir del servidor de servicio de clave la clave de red cifrada con una clave de aparato, cifrada con la clave temporal,
d) emitir la clave de red (KEY_OFFER 64) cifrada con la clave de aparato, cifrada con la clave temporal como reacción frente a la autorización de aparato (62, 72).

2. Procedimiento de acuerdo con la reivindicación 1, **caracterizado por que** la emisión de la clave de red cifrada (KEY_OFFER 64) como reacción frente a la autorización de aparato (62, 72) se realiza directamente tras la recepción de una solicitud de integración de aparato de acuerdo con la etapa a) y/o por que tras la emisión de la clave de red (KEY_OFFER 64) se vigila la recepción de un mensaje de acuse de recibo de clave (KEY_ACK 68).

3. Procedimiento de acuerdo con la reivindicación 2, **caracterizado por que** sólo tras la recepción del mensaje de acuse de recibo de clave (KEY_ACK 68) el aparato de control (22, 42) integra el aparato nuevo (2) en el sistema de automatización doméstica.

4. Procedimiento de acuerdo con una de las reivindicaciones 1 a 3, **caracterizado por que** la recepción y/o la evaluación de una solicitud de integración de aparato (INCLUSION_REQ 58) se posibilita mediante una activación (54) de un modo de integración.

5. Procedimiento de acuerdo con una de las reivindicaciones 1 a 4, **caracterizado por que** antes de la etapa a) se recibe en una etapa a0) un mensaje de búsqueda de integración (INCLUSION_DISCOVER 52) del aparato nuevo, y/o por que se determina a partir del mensaje de búsqueda de integración (INCLUSION_DISCOVER 52) una identificación de aparato del aparato nuevo (2) y/o por que tras la etapa a0) y antes de la etapa a) se emite en una etapa a1) un mensaje de oferta de integración (INCLUSION_OFFER 56) al aparato nuevo (2), y/o por que el mensaje de oferta de integración (INCLUSION_OFFER 56) emitido en la etapa a1) incluye una identificación de aparato de control y por que la solicitud de integración de aparato (INCLUSION_REQ 58) recibida en la etapa a) incluye la identificación de aparato de control.

6. Procedimiento de acuerdo con una de las reivindicaciones 1 a 5, **caracterizado por que** la clave recibida en la etapa b) está formada por al menos dos claves, siendo una primera clave una clave generada temporalmente en el aparato (2) que está cifrada con una clave almacenada permanentemente en el aparato (2).

7. Procedimiento de acuerdo con una de las reivindicaciones 1 a 6, **caracterizado por que** la autorización de aparato (62, 72) se realiza mediante una interacción de usuario o por que se consulta una identificación de aparato almacenada de manera central entre la identificación de aparato y el aparato de control (22, 42) y se realiza automáticamente una autorización en el caso de un resultado de consulta positivo.

8. Procedimiento de acuerdo con una de las reivindicaciones 5 a 7, **caracterizado por que** se activa un modo de integración del aparato de control (22, 42) mediante una interacción de usuario y por que sólo en el modo de integración se pueden evaluar y/o recibir mensajes de acuerdo con las etapas a0) y/o a) y/o por que el modo de integración se desactiva tras un tiempo definido tras la interacción de usuario.

9. Procedimiento de acuerdo con una de las reivindicaciones 1 a 8, **caracterizado por que** la clave de red se cifra con la clave temporal y, a continuación, la clave de red cifrada se transmite junto con la clave temporal en el texto claro al aparato (2).

10. Procedimiento para integrar un aparato en un sistema de automatización doméstica con las etapas de:

a) detectar un acontecimiento que activa un modo de integración (50),
b) emitir una solicitud de integración de aparato (INCLUSION_REQ 58) como reacción frente al acontecimiento, estando incluida en la solicitud de integración de aparato (INCLUSION_REQ 58) al menos una identificación de aparato,
c) recibir una clave de red (KEY_OFFER 68) cifrada con una clave de aparato, cifrada con la clave temporal,
c1) descifrar con la clave de aparato conocida en el aparato la clave de red cifrada con la clave de aparato, cifrada con la clave temporal,

c2) descifrar a continuación con la clave temporal conocida en el aparato la clave de red cifrada con la clave temporal para obtener la clave de red descifrada.

11. Procedimiento de acuerdo con la reivindicación 10, **caracterizado por que** el acontecimiento que activa el modo de integración (50) es una interacción de usuario, un encendido del aparato y/o un restablecimiento del aparato al estado de entrega, activándose el modo de integración exclusivamente para el caso de que aún no se haya recibido una clave de red (KEY_OFFER 64) en el aparato (2).

12. Procedimiento de acuerdo con las reivindicaciones 10 u 11, **caracterizado por que** la clave de red (KEY_OFFER 64) recibida se recibe junto con una identificación de aparato de control, y/o por que la clave de red (KEY_OFFER 64) recibida se confirma mediante el uso de la identificación de aparato de control con respecto al aparato de control (22, 42) con un mensaje de acuse de recibo de clave (KEY_ACK 68).

13. Procedimiento de acuerdo con una de las reivindicaciones 10 a 1, **caracterizado por que** para el caso de que ya se haya recibido una clave de red se emite un mensaje de rechazo de recepción de clave (KEY_NAK 78).

14. Aparato de control central (22, 42) para un sistema de automatización doméstica con

- una interfaz de comunicación para la recepción de una solicitud de integración de aparato (INCLUSION_REQ 58),
- un procesador para determinar al menos una identificación de aparato a partir de la solicitud de integración de aparato (INCLUSION_REQ 58),
- en el que el procesador está configurado para evaluar una autorización de aparato y para descifrar una clave de red conocida en el aparato de control con una clave temporal y activa la interfaz de comunicación para enviar la clave de red cifrada con la clave temporal junto con la identificación de aparato a un servidor de servicio de clave, y para recibir del servidor de servicio de clave la clave de red cifrada con una clave de aparato, cifrada con la clave temporal, y para emitir la clave de red (KEY_OFFER 64) cifrada con la clave de aparato, cifrada con la clave temporal como reacción frente a la autorización de aparato.

15. Aparato (2) para un sistema de automatización doméstica con:

- un procesador para detectar un acontecimiento que activa un modo de integración,
- una interfaz de comunicación para emitir una solicitud de integración de aparato (INCLUSION_REQ 58) como reacción frente al acontecimiento, estando incluida en la solicitud de integración de aparato (INCLUSION_REQ 58) al menos una identificación de aparato, y para recibir una clave de red (KEY_ACK 68) cifrada con una clave de aparato, cifrada con la clave temporal, estando el procesador configurado además para descifrar con la clave de red conocida en el aparato la clave de red cifrada con la clave de aparato, cifrada con la clave temporal, y para descifrar a continuación con la clave temporal conocida en el aparato la clave de red cifrada con la clave temporal para obtener la clave de red descifrada.

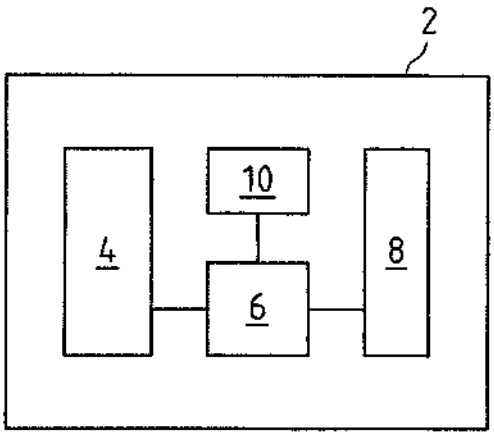


Fig.1

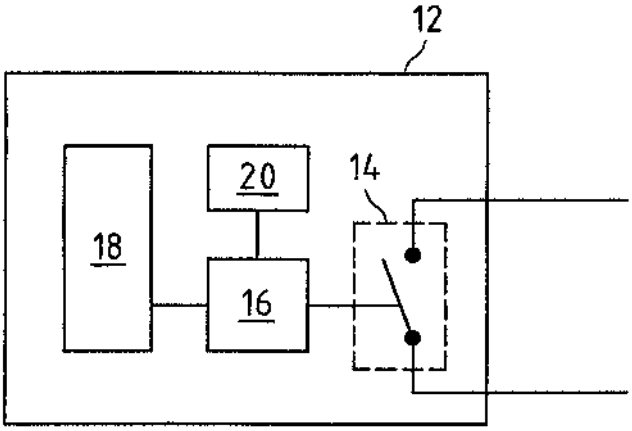


Fig.2

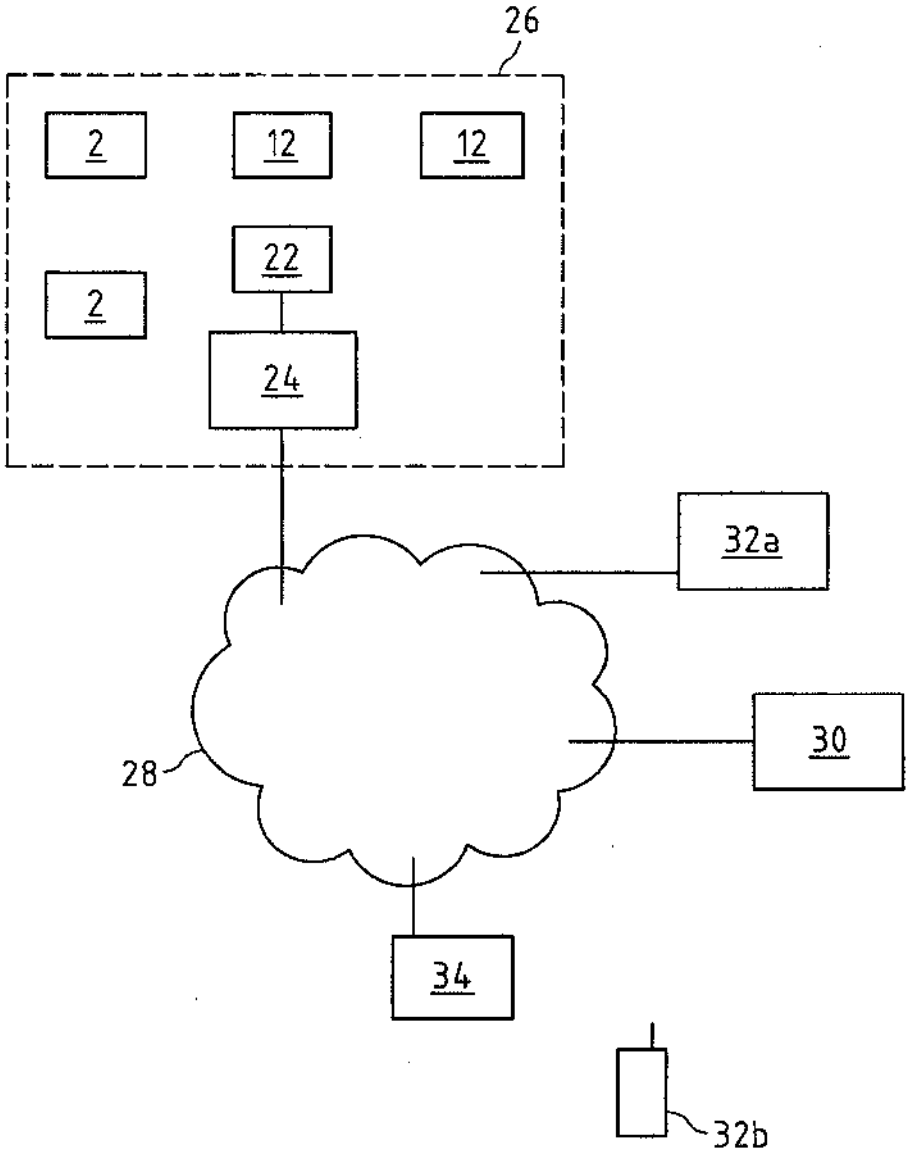


Fig.3

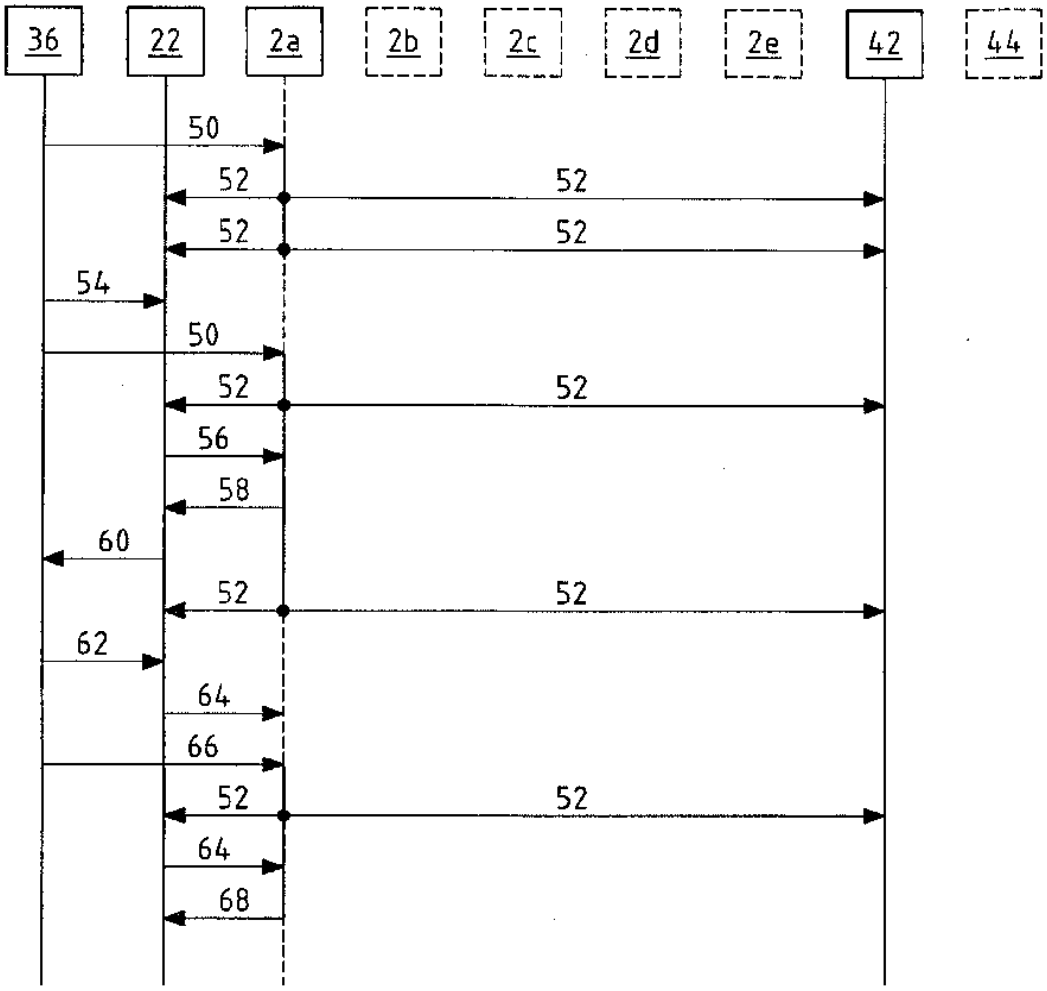
36
22
2a
2b
2c
2d
2e
42
44
50
52
52
52
52
54
50
52
52
56
58
60
52
52
62
64
66
52
52
64
68

Fig.4

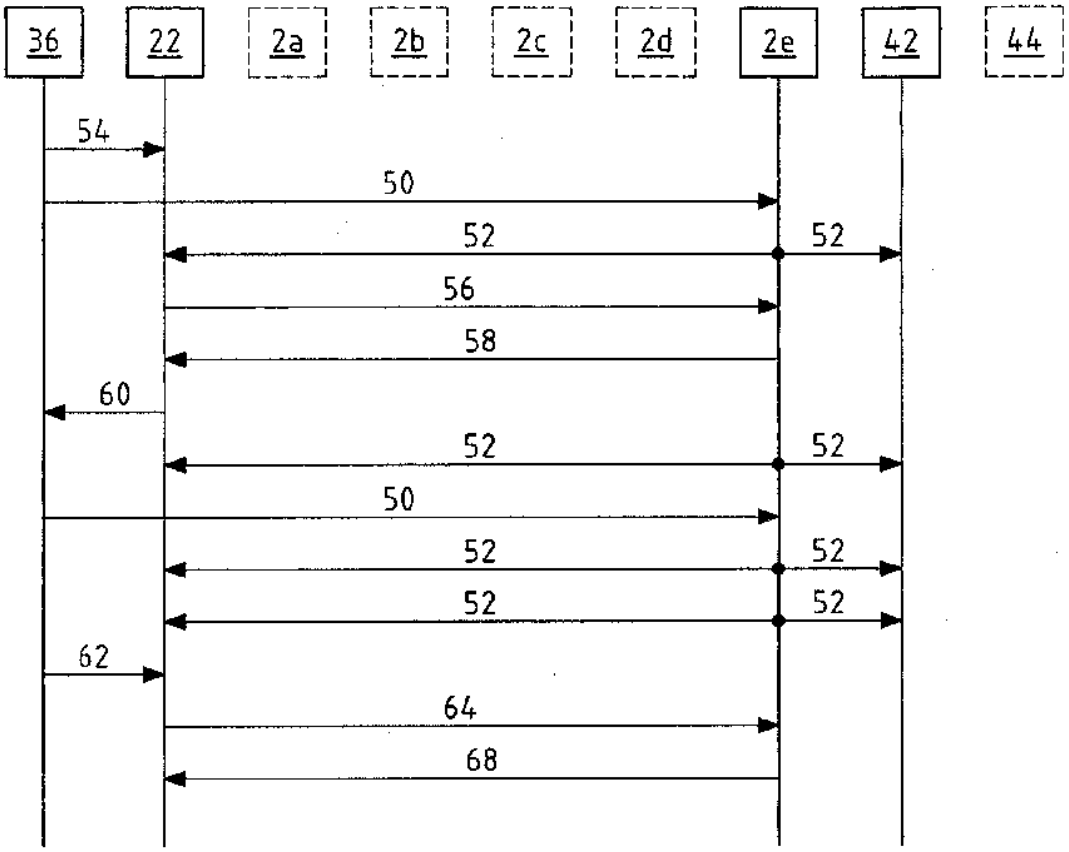
36
22
2a
2b
2c
2d
2e
42
44
54
50
52
52
56
58
60
52
52
50
52
52
52
52
62
64
68

Fig.5

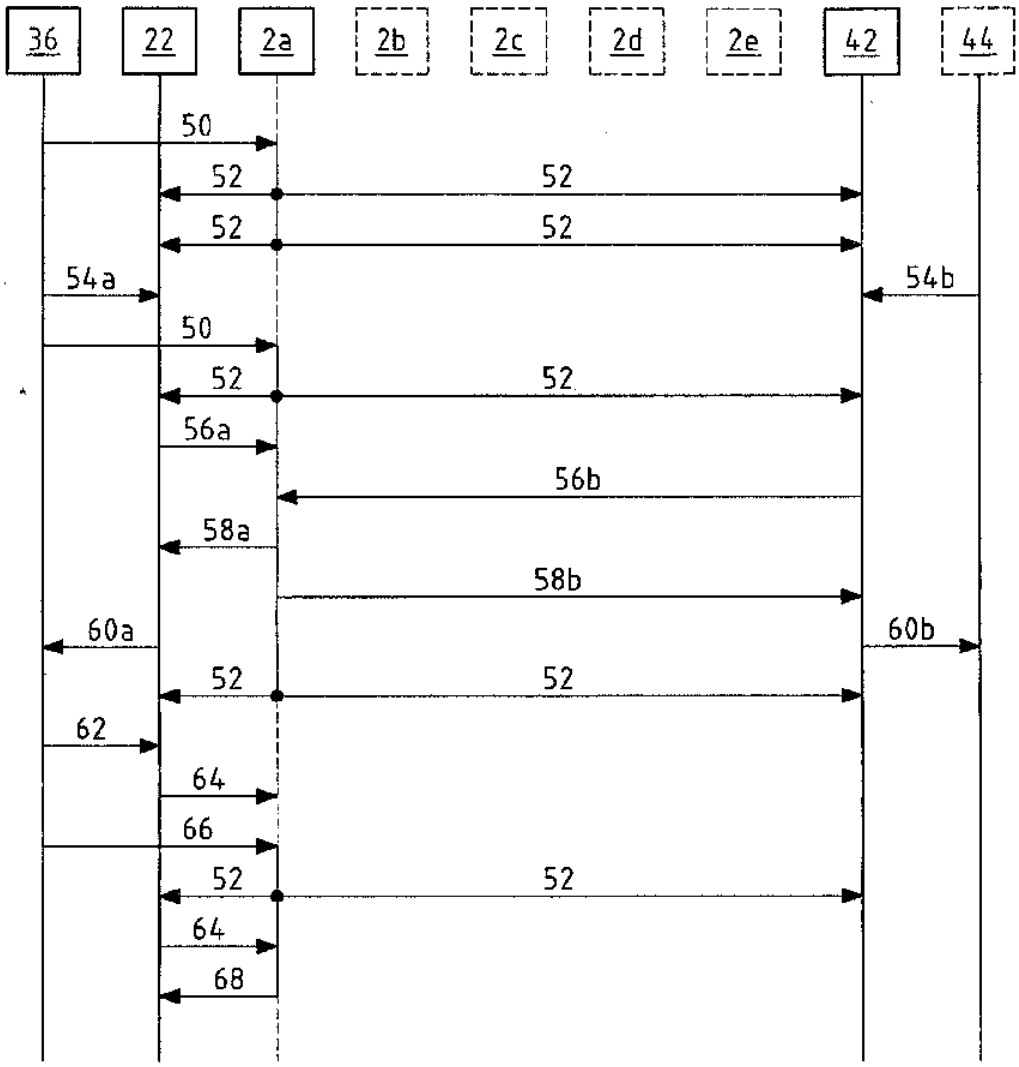
36
22
2a
2b
2c
2d
2e
42
44
50
52
52
52
52
54a
54b
50
52
52
56a
56b
58a
58b
60a
60b
52
52
62
64
66
52
52
64
68

Fig.6

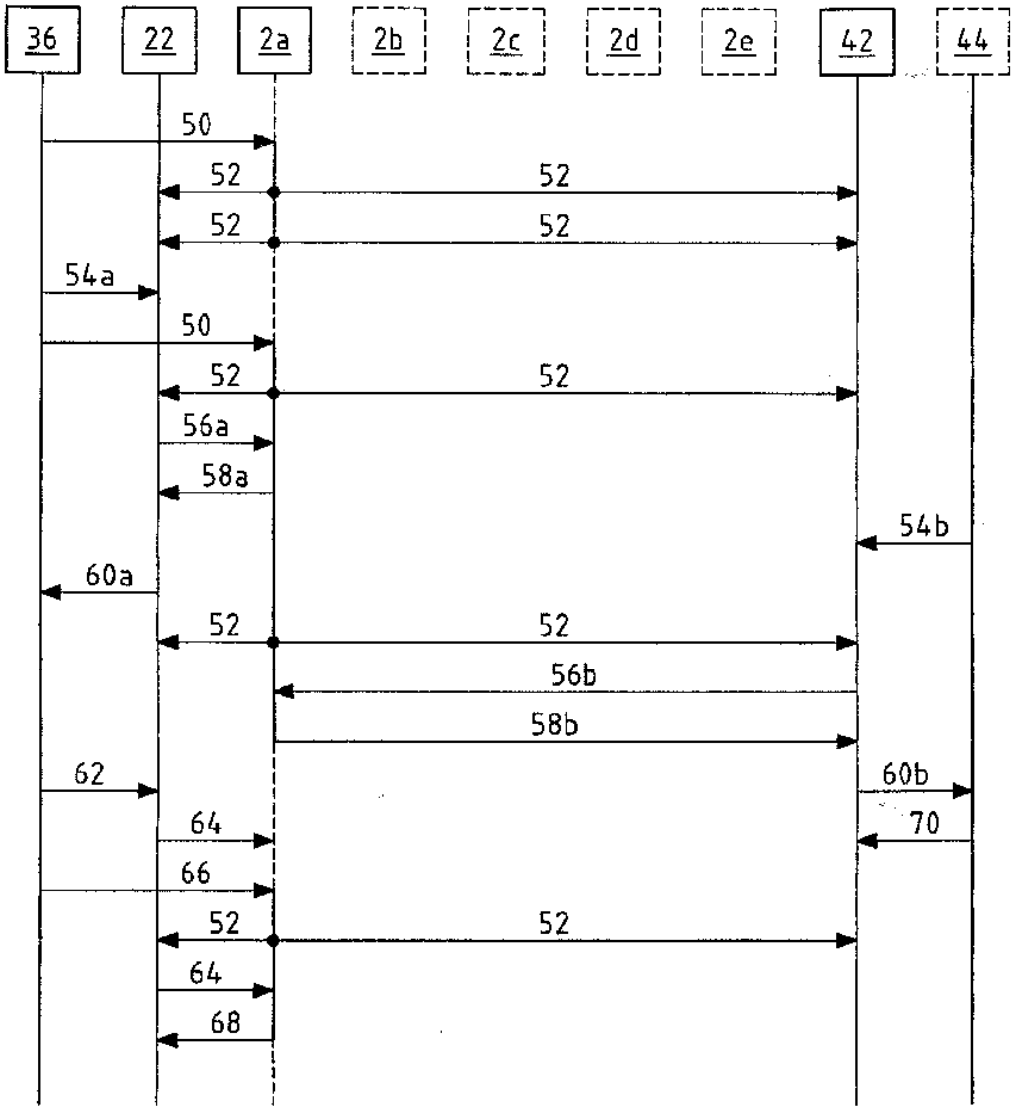
36
22
2a
2b
2c
2d
2e
42
44
50
52
52
52
52
54a
50
52
52
56a
58a
54b
60a
52
52
56b
58b
62
60b
64
70
66
52
52
64
68

Fig.7

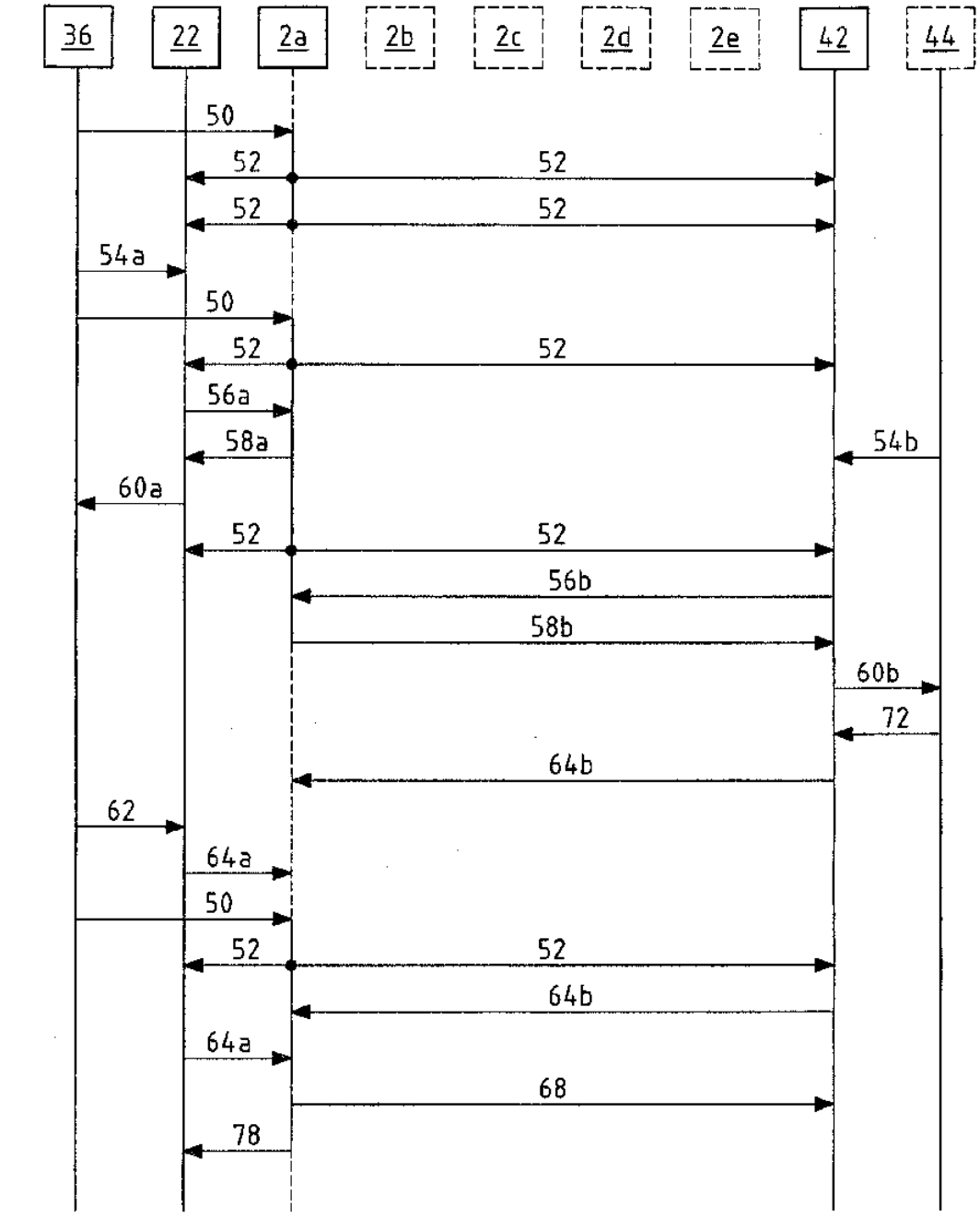
36
22
2a
2b
2c
2d
2e
42
44
50
52
52
52
52
54a
50
52
52
56a
58a
54b
60a
52
52
56b
58b
60b
72
64b
62
64a
50
52
52
64b
64a
68
78

Fig.8

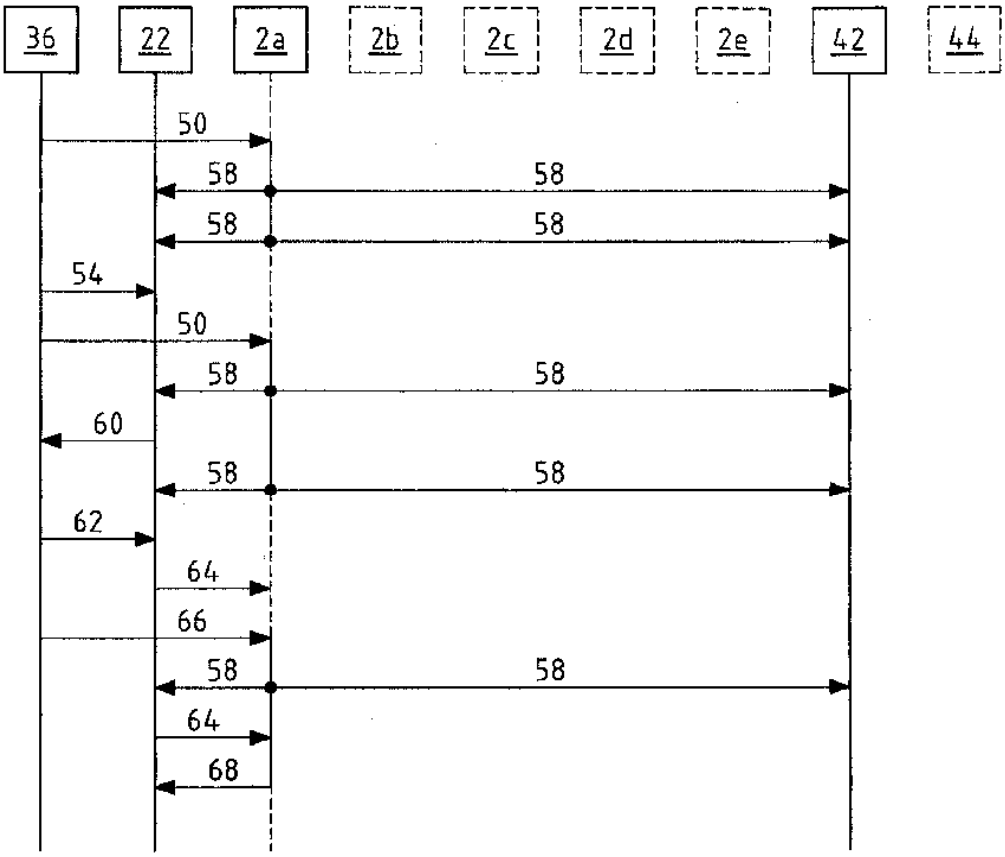
36
22
2a
2b
2c
2d
2e
42
44
50
58
58
58
58
54
50
58
58
60
58
58
62
64
66
58
58
64
68

Fig.9

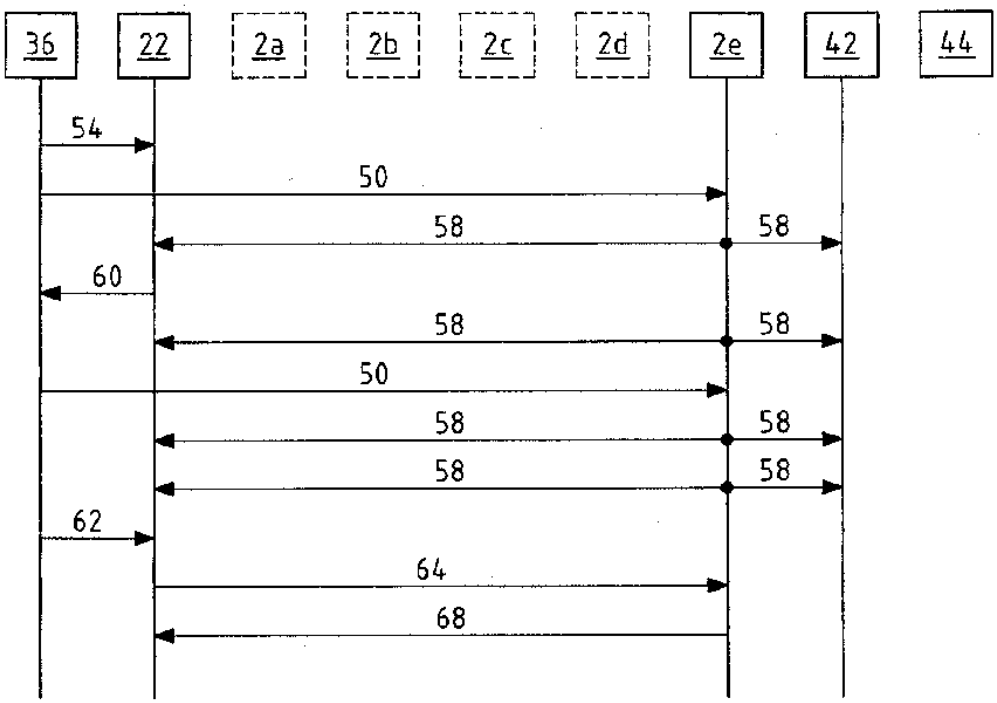


Fig.10

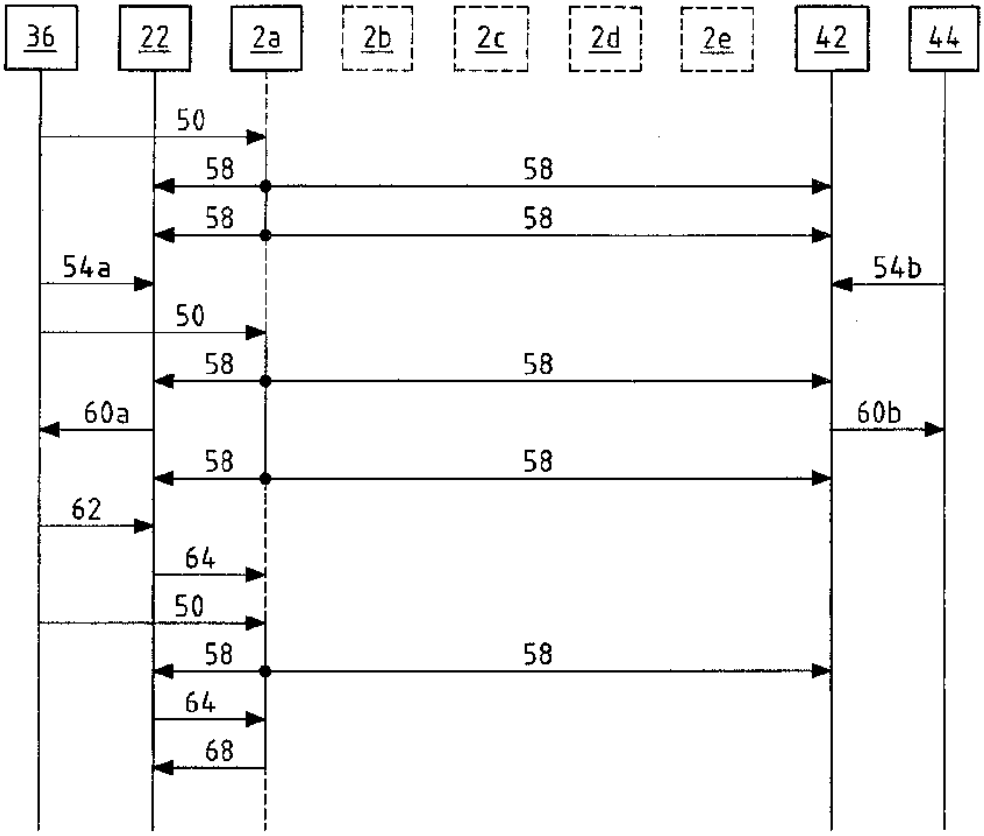
36
22
2a
2b
2c
2d
2e
42
44
50
58
58
58
58
54a
54b
50
58
58
60a
60b
58
58
62
64
50
58
58
64
68

Fig.11

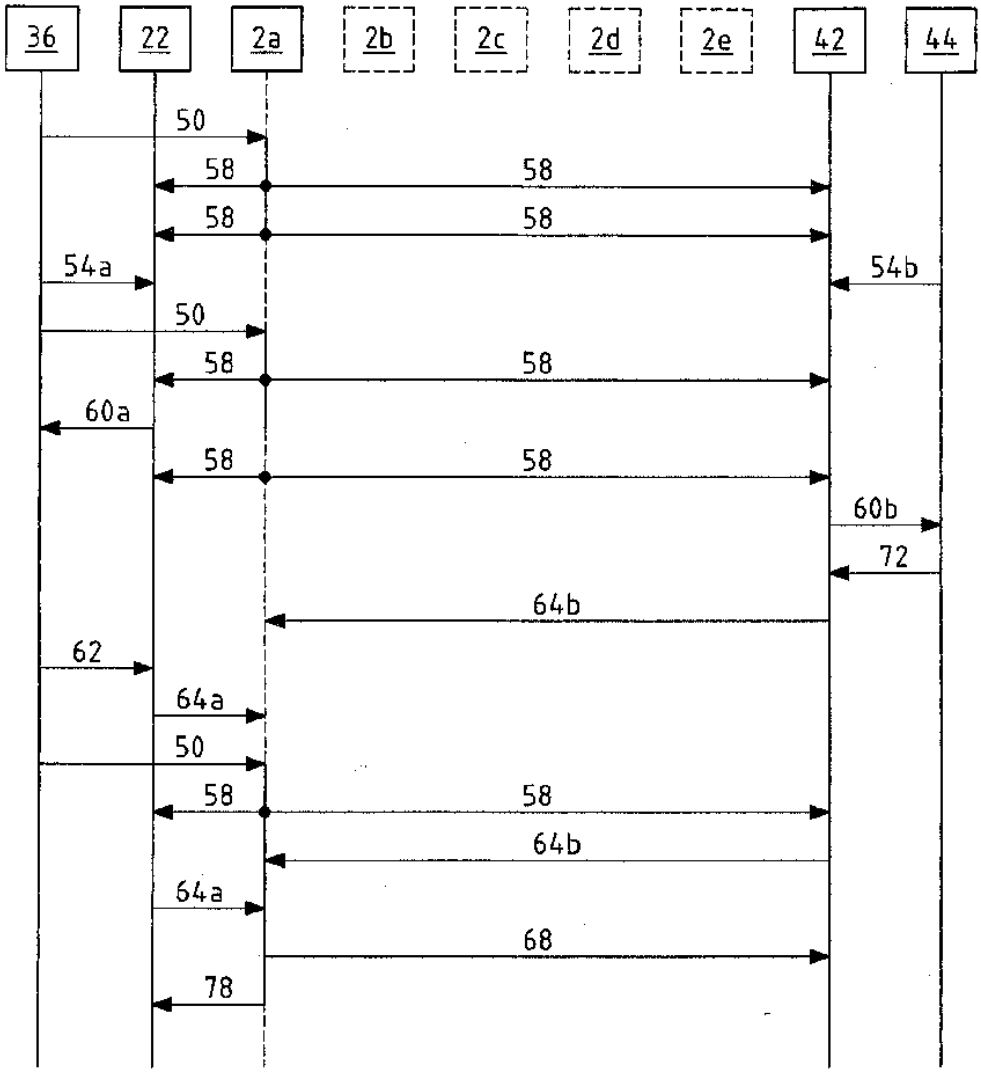
36
22
2a
2b
2c
2d
2e
42
44
50
58
58
58
58
54a
54b
50
58
58
60a
58
58
60b
72
64b
62
64a
50
58
58
64b
64a
68
78

Fig.12