(19) OFICINA ESPAÑOLA DE PATENTES Y MARCAS

ESPAÑA

(11) Número de publicación: **2 613 707**

(51) Int. CI.:

G06F 21/30 (2013.01)
G06F 21/31 (2013.01)
H04L 9/08 (2006.01)
H04L 9/32 (2006.01)
H04L 29/06 (2006.01)

(12) TRADUCCIÓN DE PATENTE EUROPEA T3

(86) Fecha de presentación y número de la solicitud internacional: **31.03.2010 PCT/EP2010/054300**

(87) Fecha y número de publicación internacional: **29.12.2010 WO2010149400**

(96) Fecha de presentación y número de la solicitud europea: **31.03.2010 E 10717073 (0)**

(97) Fecha y número de publicación de la concesión europea: **16.11.2016 EP 2446390**

(54) Título: **Sistema y procedimiento para la autentificación fiable de un aparato**

(30) Prioridad:

23.06.2009 DE 102009030019

(45) Fecha de publicación y mención en BOPI de la traducción de la patente:
25.05.2017

(73) Titular/es:

SIEMENS AKTIENGESELLSCHAFT (100.0%)
Wittelsbacherplatz 2
80333 München, DE

(72) Inventor/es:

FALK, RAINER y
FRIES, STEFFEN

(74) Agente/Representante:

LOZANO GANDIA, José

SISTEMA Y PROCEDIMIENTO PARA LA AUTENTIFICACIÓN FIABLE DE UN APARATO

DESCRIPCIÓN

La presente invención se refiere a un sistema adecuado para, en base a un enlace de una información de contexto del controlador a un mensaje de consulta, autentificar con fiabilidad un aparato, así como al correspondiente procedimiento. La invención se refiere además a un dispositivo de enlace del controlador que es adecuado para modificar un mensaje de consulta en función de una información de contexto del controlador, así como al correspondiente procedimiento. La invención se refiere además a un producto de programa de ordenador para realizar al menos uno de los procedimientos antes citados, así como a una memoria de datos que memoriza el producto de programa de ordenador.

El proceso de autentificación es en general el proceso de comprobación de una identidad. Durante este proceso se intercambian usualmente mensajes entre una unidad de prueba y un aparato que ha de autentificarse. Si un atacante intercepta estos mensajes a intercambiar, puede simular este atacante mediante los mensajes interceptados una falsa identidad. La autentificación puede servir por ejemplo para reconocer con fiabilidad un aparato, por ejemplo un sensor o una batería. En otro escenario de utilización sirve la autentificación para reconocer productos originales. También en una comunicación client-server (cliente-servidor) puede ser necesario comprobar la identidad del cliente y/o del servidor.

En procedimientos tradicionales se realiza una autentificación a menudo mediante un procedimiento challenge-response (reto-respuesta). Al aparato se le transmite entonces un mensaje de challenge, que se forma por ejemplo en función de un numero aleatorio. A continuación calcula el aparato mediante una clave criptográfica secreta un segundo valor, que también se denomina mensaje de response. Este mensaje de response se envía de retorno al generador del challenge, que a continuación comprueba si la respuesta es correcta. Puesto que sólo un producto original o bien un aparato original puede calcular un mensaje de respuesta correcto, puede diferenciarse así con fiabilidad un producto original o bien un aparato original de una falsificación.

Por el “Handbook of applied cryptography” (manual de criptografía aplicada); IDentication and entity authentication (identificación y autentificación de entidad); CRC Press; Boca Raton, págs. 385-424; ISBN: 978-0-8493-8523-0; XP002262234 de Menezes y colab, se conocen sistemas electrónicos de identificación y autentificación y los correspondientes métodos, que permiten comprobar identidades digitales. Los procedimientos challenge-response se describen allí como procedimientos de autentificación seguros y se basan en el conocimiento de un abonado, verificándose si un mensaje transmitido es correcto.

En procedimientos de autentificación tradicionales existe a menudo la necesidad de comprobar un aparato no sólo localmente, sino también a distancia mediante un puesto de comunicación, por ejemplo mediante Internet, telefonía móvil u otros enlaces de datos. Esta necesidad existe en particular en un mantenimiento a distancia del aparato. En una comprobación a distancia de una identidad aparece a menudo el problema de que una entidad intermedia puede leer mensajes y utilizarlos para simular una identidad falsa. Este escenario de ataque se conoce como ataque Man-in-the-Middle (intermediario).

En procedimientos tradicionales se utiliza una autentificación RFID-Tag (etiqueta RFID) simétrica. Aquí se utilizan chips, que ejecutan operaciones criptográficas y con ello reconocen con fiabilidad un producto original.

Un sistema criptográfico asimétrico está compuesto por varias entidades que se comunican entre sí, poseyendo cada una de las entidades que comunican un par de claves, compuesto por una parte secreta y una parte no secreta. Los procedimientos criptográficos asimétricos se conocen también como procedimientos Public-Key (de clave pública).

Además se utilizan en procedimientos tradicionales los llamados métodos Keybinding (de clave ligada). En ellos se liga una clave criptográfica a una determinada finalidad de utilización. Esto se realiza en procedimientos tradicionales por ejemplo mediante una deducción de clave por medio de una función de deducción de clave, que utiliza como parámetro de entrada, además de la clave no ligada a una finalidad, una cadena de caracteres que describe la finalidad de utilización que se pretende. Como ejemplo de ello se calcula en WiMAX a partir de una clave no ligada a la finalidad EMSK primeramente una clave Mobile-IP-Root y a partir de ello se calculan otras claves IP móviles ligadas a la finalidad.

Además se utilizan en procedimientos tradicionales protocolos de seguridad de la red, para proteger criptográficamente una comunicación basada en IP. Entonces se realiza un autentificación de los interlocutores de comunicación tanto por un lado como también mutuamente. Son protocolos utilizados a menudo, que realizan una autentificación de un interlocutor de comunicación, los conocidos como SSL, TLS o IKE para IPsec. La autentificación de un interlocutor de comunicación, especialmente de un servidor http mediante SSL o TLS, se realiza entonces mediante un certificado digital. Este certificado contiene, además de la clave pública del servidor, también denominada Public-Key, información sobre el servidor, en particular su denominación, como por ejemplo nombre, nombre DNS o dirección de IP.

Igualmente por procedimientos tradicionales se conoce el protocolo Kerberos, con cuya ayuda puede realizarse la autentificación y la autorización mediante un tercero digno de confianza. Kerberos se basa en la utilización de claves simétricas.

La figura 1 representa el servicio de autentificación Kerberos según un procedimiento tradicional. Kerberos es un servicio de autentificación distribuido o bien un protocolo de red que se desarrolló para redes de ordenadores abiertas e inseguras, como por ejemplo Internet. La autentificación la asume según Kerberos un tercero digno de confianza, por ejemplo un servidor Kerberos.

Según el procedimiento Kerberos descrito en la figura 1, solicita un usuario o User N en una primera etapa mediante un mensaje de solicitud o un Request R-TG-T un Ticket-Granting-Ticket (ticket para conseguir tickets) mediante un mensaje R-TG-T de un servidor Kerberos KS. Un ticket es aquí un mensaje de autorización con el que el correspondiente poseedor del mensaje obtiene acceso al servidor S. En una etapa siguiente transmite el servidor Kerberos KS un ticket T y una Ticket-Granting-Session-Key (clave de sesión para conseguir tickets) TGSK al User N. Para transmitir ambos mensajes Ticket T y Ticket-Granting-Session-Key TGSK dispone el servidor Kerberos KS de un Key Distribution Service (servicio de distribución de claves) KDS. Este servicio de distribución de claves KDS comunica mediante un enlace de datos con el banco de datos DB.

En una etapa del procedimiento que va a continuación solicita el usuario N un Service-Grant-Ticket SGT, para lo cual accede el Kerberos-Server KS a un Ticket-Granting-Server TGS. A continuación transmite el Ticket-Granting-Server TGS un mensaje de Ticket T, así como una Session-Key (clave de sesión) SK al usuario N. En función de los mensajes recibidos crea el usuario N un mensaje Request Service (solicitud de servicio) RS y lo transmite a otro servidor S. En función de la comprobación del mensaje Request Service RS transmite este servidor S un mensaje Server Authenticator (autentificación de servidor) al usuario N.

Otro ejemplo de protocolo de red según un procedimiento tradicional es SAML, también conocido como Secure Assertion Mark-up Language (lenguaje de marcado para confirmaciones de seguridad). A diferencia de Kerberos, pueden utilizarse en SAML también métodos asimétricos.

La figura 2 describe una autentificación de aparato según un procedimiento tradicional.

La figura 2 muestra en una representación esquemática el intercambio de mensajes entre un aparato lector RFID, RFID-LG y un tag RFID, RFID-T según un procedimiento criptográfico asimétrico. Aquí se representa una autentificación unilateral del tag RFID, RFID-T. Según una consulta A (getcertificate) del aparato lector RFID, RFID-LG, envía el tag RFID su certificado al aparato lector RFID, RFID-LG. El certificado del tag RFID, RFID-T, presenta la clave pública del tag RFID. La aportación y/o el envío de la clave pública se realiza/n por ejemplo en un mensaje Public Key Signature (firma de clave pública) PKSN. El certificado del tag RFID, RFID-T, presenta una firma de un expedidor de certificados. En el caso de que el aparato lector RFID, RFID-LG, no pueda verificar con éxito el certificado del tag RFID, RFID-T, se detecta el tag RFID, RFID-T, como no original, lo cual origina una interrupción del procedimiento. Si se reconoce el certificado como válido, genera el aparato lector RFID, RFID-LG, un mensaje de consulta de challenge aleatorizado y lo envía al tag RFID. El tag RFID, RFID-T, calcula un mensaje response Re en función de una clave privada del tag RFID, RFID-T. Este mensaje response Re se envía al aparato lector RFID, RFID-LG. El aparato lector RFID, RFID-LG, verfica el mensaje response Re utilizando la clave pública del tag RFID, RFID-T. En función de esta verificación, se acepta el tag RFID, RFID-T, o se rechaza, es decir, se detecta como original o como falsificación.

La figura 3 describe un escenario de ataque en una autentificación según un procedimiento tradicional. La presente figura 3 sirve para mostrar un ataque Man-in-the-Middle según un procedimiento tradicional de autentificación challenge-response. Un servidor 33 autentifica un aparato 31 utilizando una unidad de autentificación 30. Para ello solicita el servidor 33 un certificado Z del aparato 31 mediante un mensaje Get_Device_Cert (obtener certificado del aparato) GDC. En el ejemplo representado ha conseguido un atacante 32 conectarse en el flujo de mensajes entre el servidor 33 y el aparato 31, es decir, interceptar el intercambio de mensajes entre el servidor 33 y el aparato 31. La unidad de autentificación 30 transmite según la consulta un certificado Z en un mensaje Cert, Cert, al servidor 33. En una subsiguiente etapa del procedimiento S1 genera el servidor 33 un challenge (reto) Ch o mensaje de consulta en función del cual la unidad de autentificación 30 calcula un mensaje response Re. El cálculo del mensaje response Re puede realizarse en función de la ejecución de un método de autentificación del aparato AD(Ch). La verificación del mensaje response Re puede realizarse en función de la ejecución de un método de autentificación de la respuesta ADR(Re). El servidor 33 verifica en una etapa S2 si el mensaje response Re, calculado mediante la unidad de autentificación 30, es válido respecto al mensaje response esperado según el mensaje challenge Ch.

Así ha autentificado el servidor 33 al aparato 31 con éxito en el escenario de ataque descrito en la figura 3, pero habiendo reenviado el atacante 32 los mensajes del servidor 33 solamente al aparato 31. El servidor 33 presupone incorrectamente que él mismo comunica con un aparato original. No obstante, el atacante 32 puede utilizar otro aparato original para calcular un mensaje response de autentificación de aparato válido.

Los métodos tradicionales para autentificar aparatos no son a menudo fiables y sólo pueden llevarse a cabo con un considerable coste en recursos. La falta de fiabilidad del procedimiento tradicional puede resultar en particular en función de la creación del mensaje challenge o mensaje de consulta. Además se necesitan en el procedimiento

tradicional una pluralidad de entidades, que aumentan fuertemente la necesidad de recursos. Además una pluralidad de entidades participantes puede originar una falta de fiabilidad del procedimiento de autentificación utilizado, ya que los mensajes intercambiados entre la pluralidad de entidades pueden ser interceptados y/o falsificados.

Por lo tanto es un objetivo de la presente invención proporcionar un sistema mejorado y/o un dispositivo mejorado para la autentificación fiable de un aparato o bien para modificar un mensaje de consulta en función de una información de contexto del controlador.

Este objetivo se logra mediante un sistema para la autentificación fiable de un aparato de acuerdo con la reivindicación 1. En consecuencia se prevé un sistema para la autentificación fiable de un aparato con:

> un dispositivo de prueba, que en función de un mensaje de respuesta verifica una identidad del aparato, calculando el aparato el mensaje de respuesta en función de un mensaje de consulta modificado y un dispositivo de enlace del controlador calcula el mensaje de consulta modificado en función de una información de contexto proporcionada y un mensaje proporcionado.

Una autentificación de un aparato puede ser por ejemplo una comprobación de autenticidad de un sensor o de una batería. Un aparato puede también estar configurado como dispositivo virtual. Así es adecuado el sistema correspondiente a la invención para la autentificación fiable de un cliente (client) y/o de un servidor (server). El dispositivo de prueba puede existir por ejemplo como un servidor, que comprueba la identidad de un aparato client. El dispositivo de prueba puede existir por ejemplo como una unidad de cálculo virtual, un servidor virtual y/o servidor físico. El intercambio de mensajes entre el dispositivo de prueba, el dispositivo de enlace del controlador y el aparato puede realizarse mediante un enlace de datos. El enlace de datos puede presentar entonces otros componentes típicos de la red.

El dispositivo de prueba es adecuado para crear el mensaje de consulta, también denominado mensaje challenge (de reto) y transmitirlo al dispositivo de enlace del controlador. La creación del mensaje de consulta puede realizarse por ejemplo en función de un número aleatorio o número pseudoaleatorio generado por el dispositivo de prueba. A continuación transmite el dispositivo de prueba una información de contexto del controlador al dispositivo de enlace del controlador. El dispositivo de enlace del controlador calcula en función de la información de contexto del controlador transmitida y del mensaje de consulta un mensaje de consulta modificado. El cálculo del mensaje de consulta modificado puede realizarse mediante la función Context-Binding (de enlace del contexto). La función Context-Binding puede existir como una función de derivación de clave, que utiliza la información de contexto del controlador y el mensaje de consulta proporcionado como parámetros de entrada.

El mensaje de consulta modificado calculado se transmite en una forma de realización al aparato, que en función del mensaje de consulta modificado crea un mensaje de respuesta, también denominado mensaje response. La creación del mensaje response puede realizarse utilizando una clave criptográfica. Tras el cálculo del mensaje response, se transmite el mismo mediante el dispositivo de enlace del controlador al dispositivo de prueba. El dispositivo de prueba es adecuado para calcular la clave modificada en función de la información de contexto del controlador proporcionada y del mensaje de consulta proporcionado. La creación del mensaje de consulta modificado mediante el dispositivo de prueba puede realizarse análogamente a la creación del mensaje de consulta modificado mediante el dispositivo de enlace del controlador. Aquí pueden utilizarse por lo tanto en ambos cálculos la misma función Context-Binding y/o los mismos parámetros de entrada. En función del mensaje de consulta modificado calculado por el dispositivo de prueba, es adecuado el dispositivo de prueba para verificar el mensaje response proporcionado por el aparato. Esto se realiza por ejemplo mediante una función Response-Verification (de verificación de respuesta), que utiliza el mensaje response proporcionado y/o el mensaje de consulta modificado creado por el dispositivo de prueba como parámetro de entrada.

Si el mensaje response proporcionado por el aparato significa una respuesta al mensaje de consulta proporcionado por el dispositivo de prueba según el procedimiento Challenge-Response ya descrito, se reconoce el aparato como aparato original. Esto significa que el aparato existe como el interlocutor de comunicación contemplado efectivamente por el dispositivo de prueba y la identidad del aparato queda autentificada.

En una forma de realización del sistema de acuerdo con la invención, se crea la información de contexto del controlador en función de al menos una característica del dispositivo de prueba.

Esto tiene la ventaja de que el mensaje de consulta modificado se calcula en función de un mensaje de consulta ya aportado y al menos un parámetro adicional, que es la información de contexto del controlador. Además esto tiene la ventaja de que el dispositivo de prueba verifica un mensaje response que ha sido calculado en relación con un mensaje de consulta que acaba de calcular este dispositivo de prueba. Esto contribuye esencialmente a una autentificación fiable del aparato.

En otra forma de realización del sistema de acuerdo con la invención, presenta el dispositivo de prueba una característica de identidad, una dirección de IP, un nombre de ordenador, una dirección MAC, un certificado, una clave de sesión, una clave y/o un token de autentificación.

Esto tiene la ventaja de que la información de contexto del controlador puede crearse en función exactamente de estas características del dispositivo de prueba. Puesto que estas características se refieren al dispositivo de prueba, no puede imitar la información de contexto del controlador una tercera entidad, en particular un atacante.

En otra forma de realización del sistema de acuerdo con la invención, presenta el dispositivo de prueba una unidad de aportación de la información de contexto del controlador, para proporcionar informaciones de contexto del controlador y/o una unidad de aportación de mensajes de consulta, para proporcionar el mensaje de consulta.

Esto tiene la ventaja de que el dispositivo de prueba puede calcular autónomamente tanto las informaciones de contexto del controlador como también el mensaje de consulta. Así pueden integrarse otros mecanismos de seguridad en el sistema propuesto.

En otra forma de realización del sistema de acuerdo con la invención proporciona el dispositivo de gestión de claves KDC la información de contexto del controlador y/o el mensaje de consulta.

Esto tiene la ventaja de que la información de contexto del controlador y/o el mensaje de consulta puede proporcionarlos una tercera unidad, por ejemplo que tenga especial credibilidad. En consecuencia pueden encontrar utilización también en el sistema propuesto mecanismos de seguridad ya implementados.

En otra forma de realización del sistema de acuerdo con la invención, presenta el dispositivo de enlace del controlador una primera unidad de modificación de consulta, que calcula el mensaje de consulta modificado según una función de derivación de clave en dependencia de la información de contexto del controlador y del mensaje de consulta.

Esto ofrece la ventaja de que pueden utilizarse funciones de derivación de claves ya implementadas para calcular el mensaje de consulta modificado. Además esto tiene la ventaja de que el dispositivo de enlace del controlador puede codificar el mensaje de consulta proporcionado en función de la información de contexto del controlador.

En otra forma de realización del sistema de acuerdo con la invención verifica el dispositivo de prueba el mensaje de respuesta mediante una segunda unidad de modificación de consulta y una unidad de verificación de respuesta, calculando la segunda unidad de modificación de consulta el mensaje de consulta modificado según la función de derivación de claves y verificando la unidad de verificación de respuesta el mensaje de respuesta en función del mensaje de consulta modificado calculado.

Al respecto puede realizarse la comprobación o la verificación del mensaje de respuesta utilizando la misma clave criptográfica, también denominada criptografía de clave secreta (secret-key) o bien una segunda clave asociada a la primera clave criptográfica, también denominada criptografía de clave pública (public-key).

Esto tiene la ventaja de que la verificación del mensaje response o del mensaje de respuesta se realiza en función de una unidad de consulta modificada calculada por el dispositivo de prueba.

En otra forma de realización del sistema de acuerdo con la invención elige una unidad de elección la función de derivación de claves a partir de un conjunto de funciones de derivación de claves memorizadas en una memoria de datos y proporciona la función de derivación de claves elegida al menos a una de las unidades de modificación de consultas.

Esto tiene la ventaja especial de que puede elegirse una función de derivación de claves a partir de una pluralidad de funciones de derivación de claves. Al respecto puede utilizarse ventajosamente en la primera y también la segunda unidad de modificación de consulta la misma unidad de derivación de claves.

En otra forma de realización del sistema de acuerdo con la invención presenta el conjunto memorizado de funciones de derivación de claves procedimientos basados en MD5, SHA-1, SHA-256, SHA-512, HMAC y/o CRC32.

Esto tiene la ventaja de que la función de derivación de claves puede elegirse a partir de una pluralidad de funciones de derivación de claves conocidas.

En otra forma de realización del sistema de acuerdo con la invención transmite el aparato el mensaje de respuesta calculado al dispositivo de enlace del controlador y el dispositivo de enlace del controlador transmite el mensaje de respuesta calculado al dispositivo de prueba.

Esto ofrece la ventaja de que se transmiten el mensaje de consulta y el mensaje de respuesta desde la misma entidad en cada caso, que es el dispositivo de enlace del controlador, al dispositivo de prueba.

En otra forma de realización del sistema de acuerdo con la invención, transmite el aparato el mensaje de respuesta calculado al dispositivo de prueba.

Esto genera la ventaja de que el aparato transmite el mensaje de respuesta calculado directamente al dispositivo de prueba.

El objetivo se logra además mediante un dispositivo de enlace del controlador para modificar un mensaje de consulta en función de una información de contexto del controlador con:

- una interfaz de información de contexto del controlador para recibir y proporcionar la información de contexto del controlador a una unidad de enlace del controlador;
- una interfaz de mensajes de consulta para recibir y proporcionar un mensaje de consulta a la unidad de enlace del controlador y
- la unidad de enlace del controlador, que calcula un mensaje de consulta modificado en función de las informaciones de contexto del controlador proporcionadas y del mensaje de consulta proporcionado.

El dispositivo de enlace del controlador propuesto puede encontrar aplicación en un sistema según los ejemplos de realización antes citados.

La invención se refiere además a un procedimiento para la autentificación fiable de un aparato, en particular para operar un sistema según uno de los ejemplos de realización antes citados, con las etapas:

- cálculo de un mensaje de consulta modificado en función de una información de contexto del controlador proporcionada y de un mensaje de consulta proporcionado;
- cálculo de un mensaje de respuesta en función de un mensaje de consulta modificado y
- verificación de una identidad de un aparato en función del mensaje de respuesta calculado.

La invención se refiere además a un procedimiento para modificar un mensaje de consulta en función de una información de contexto del controlador, en particular para operar un dispositivo de enlace del controlador según uno de los ejemplos de ejecución antes descritos, con las etapas:

- aportación de la información de contexto del controlador a una unidad de enlace del controlador;
- aportación del mensaje de consulta para la unidad de enlace del controlador y
- cálculo de un mensaje de consulta modificado en función de la información de contexto del controlador proporcionada y del mensaje de consulta proporcionado.

La invención se refiere además a un producto de programa de ordenador para operar un sistema según una de las formas de realización antes citadas y/o para operar uno de los dispositivos de enlace del controlador antes citados.

La invención se refiere además a una memoria de datos que memoriza el producto de programa de ordenador antes citado.

La invención logra así un sistema y un dispositivo de enlace del controlador, incluyendo el correspondiente procedimiento, que permiten, mediante un enlace de un mensaje de consulta a un dispositivo de prueba, realizar una autentificación segura de un aparato. El enlace del mensaje de consulta al dispositivo de prueba se realiza de acuerdo con la invención mediante el dispositivo de enlace del controlador para modificar un mensaje de consulta en función de una información de contexto del controlador.

Otras variantes ventajosas de la invención son objeto de las reivindicaciones secundarias, así como de los ejemplos de realización descritos a continuación.

A continuación se describirá la invención más en detalle en base a implementaciones a modo de ejemplo, con referencia a las figuras adjuntas.

Se muestra al respecto en:

figura 1 un protocolo de autentificación según un procedimiento tradicional;
figura 2 un intercambio de mensajes esquemático según un procedimiento tradicional challenge-response;
figura 3 un escenario de ataque según un procedimiento tradicional Man-in-the Middle;
figura 4 un sistema para autentificar con fiabilidad un aparato según un ejemplo de realización de la presente invención;
figura 5 un dispositivo de enlace del controlador para modificar un mensaje de consulta según un ejemplo de realización de la presente invención;
figura 6 un procedimiento para autentificar con fiabilidad un aparato según un ejemplo de realización de la presente invención;
figura 7 una descripción detallada de un procedimiento para autentificar con fiabilidad un aparato según un ejemplo de realización de la presente invención;
figura 8 un procedimiento para modificar un mensaje de consulta en función de una información de contexto del controlador según un ejemplo de realización de la presente invención;
figura 9 un diagrama secuencial de un procedimiento para autentificar con fiabilidad un aparato según un ejemplo de realización de la presente invención y
figura 10 un diagrama secuencial de un procedimiento para autentificar con fiabilidad un aparato con una unidad de distribución de claves según un ejemplo de realización de la presente invención.

En las figuras están dotados los mismos elementos o elementos que realizan la misma función de las mismas referencias, siempre que no se indique otra cosa.

La figura 4 describe un sistema para autentificar con fiabilidad un aparato 42. El sistema presenta un dispositivo de prueba 40, que en función de un mensaje de respuesta R recibido verifica la identidad del aparato 42. El aparato 42 calcula el mensaje de respuesta R en función de un mensaje de consulta modificado C'. Además está previsto un dispositivo de enlace del controlador 41, que calcula un mensaje de consulta modificado C' en función de una información de contexto del controlador K proporcionada por el dispositivo de prueba 40 y un mensaje de consulta C proporcionado por el dispositivo de prueba 40.

El dispositivo de prueba 40 presenta en una forma de realización una unidad de aportación de información de contexto del controlador 40A, que genera la información de contexto de prueba K. La unidad de aportación de información de contexto del controlador 40A es adecuada para determinar características o features del dispositivo de prueba 40 y/o leer estas características de una memoria de datos. Estas características incluyen por ejemplo una característica de identidad ID, una dirección de IP, un nombre de ordenador, una dirección MAC, un certificado, una clave de sesión (session-key), una clave o un token de autentificación del dispositivo de prueba 40.

Para generar la información de contexto del controlador K mediante la unidad de aportación de la información de contexto del controlador 40A, son especialmente adecuadas características de un servidor, pudiendo actuar el dispositivo de prueba 40, el dispositivo de enlace del controlador 41, el aparato 42 o un servicio de autentificación como servidor. La información de contexto del controlador puede calcularse en función de al menos una de las siguientes características:

- una identidad del servidor (Server-Identity), por ejemplo una dirección de IP, un nombre de ordenador DNS, una dirección MAC, siempre que la unidad del controlador y la unidad de autentificación se encuentren en la misma subred, es decir, que las mismas utilicen las direcciones MAC propias para el direccionamiento y no aquéllas de un enrutador;
- un certificado del servidor o bien un campo o varios campos del certificado del servidor; especialmente la clave pública del servidor (Server-Public-Key) o también una huella dactilar (fingerprint) del certificado, que se calcula mediante una función hash;
- una clave de sesión (Session Key) o bien un valor derivado de la misma de la sesión de seguridad acordada mediante el protocolo de seguridad de la red;
- una clave previamente compartida (preshared) o bien la derivación de una clave previamente compartida entre una unidad del controlador y una unidad de autentificación;
- un token de autentificación, con el que el servidor se ha autentificado previamente;
- si se realiza una autentificación mutua, pueden también considerarse a la vez la identidad del cliente o también el certificado del cliente o partes de los mismos y/o
- un número aleatorio, creado mediante la unidad de aportación de información de contexto del controlador 40A.

En otra forma de realización presenta el dispositivo de prueba 40 una segunda unidad de modificación de consulta 40C. Entonces puede corresponder la unidad de modificación de consulta 40C a la unidad de modificación de consulta 41A del dispositivo de enlace del controlador 41. Entonces se encuentran ambas unidades de modificación de consulta 40C y 41A con preferencia como dos unidades separadas. Ambas unidades de modificación de consulta 40C y la unidad de modificación de consulta 41A pueden comunicar con una unidad de elección, que proporciona una función de derivación de claves para calcular el mensaje de consulta modificado.

El aparato 42 es adecuado para deducir mediante una unidad de aportación de mensajes de respuesta 42A, a partir del mensaje de consulta modificado C', un mensaje de respuesta o un mensaje response R. Para deducir el mensaje response R del mensaje de consulta modificado C', pueden utilizarse por ejemplo procedimientos tradicionales de derivación de claves.

El mensaje response R generado por el aparato 42 se envía a una unidad de verificación 40D, que por ejemplo está prevista en el dispositivo de prueba 40. La unidad de verificación 40D es adecuada para determinar, en base al mensaje response R recibido y al mensaje de consulta modificado C', si el mensaje response R recibido por el aparato 42 coincide con la respuesta esperada al mensaje de consulta modificado C'. En caso de coincidencia, se autentifica positivamente el aparato 42, es decir, el aparato 42 ha enviado de retorno el mensaje response R esperado.

La figura 5 representa un dispositivo de enlace del controlador 41 para modificar un mensaje de consulta C en función de una información de contexto del controlador K con:

una interfaz de información de contexto del controlador 41B para recibir la información de contexto del controlador K y para proporcionarla a una unidad de enlace del controlador 41A. El dispositivo de enlace del controlador 41 contiene además una interfaz de mensajes de consulta 41C para recibir el mensaje de consulta y para proporcionarlo a la unidad de enlace del controlador 41A. La unidad de enlace del controlador 41A calcula un mensaje de consulta modificado C' en función de la información de contexto del controlador K proporcionada y del mensaje de consulta C proporcionado.

El dispositivo de enlace del controlador 41 descrito en la presente figura 5 encuentra aplicación por ejemplo en un sistema como el de la figura 4.

La figura 6 muestra un diagrama secuencial de un procedimiento para autentificar con fiabilidad un aparato 42, en particular para operar un sistema como el de la figura 4. El procedimiento incluye al respecto las siguientes etapas:

En una etapa 100 se calcula un mensaje de consulta modificado C' en función de una información de contexto del controlador K proporcionada y de un mensaje de consulta C proporcionado.

A continuación se calcula en una etapa 101 un mensaje de respuesta R en función del mensaje de consulta modificado C'.

A continuación se realiza en una etapa 102 la verificación de la identidad del aparato 42 en función del mensaje de respuesta R.

Las etapas del procedimiento descritas pueden realizarse iterativamente y/o en otra secuencia.

La figura 7 describe un diagrama secuencial detallado de un procedimiento para autentificar con fiabilidad un aparato 42.

En una etapa del procedimiento de preparación 200 se realiza la preparación del mensaje challenge C mediante el dispositivo de prueba 40 al dispositivo de enlace del controlador 41. La aportación del mensaje challenge C puede presentar otras etapas subordinadas, como por ejemplo la generación del mensaje de challenge C. El mensaje de challenge C puede por ejemplo generarse en función de un número aleatorio o número pseudoaleatorio. El mensaje challenge C puede estar compuesto también por varias informaciones individuales. Por ejemplo pueden presentar el mensaje challenge C una marca de tiempo.

En una etapa siguiente 201 del procedimiento proporciona la información de contexto del controlador K el dispositivo de prueba 40 al dispositivo de enlace del controlador 41. La aportación de la información de contexto del controlador K puede incluir otras etapas subordinadas, como por ejemplo la generación de la información de contexto del controlador K. La generación de la información de contexto del controlador K puede incluir además la lectura de características del dispositivo de prueba 40.

Alternativamente a la aportación del mensaje de challenge C descrita en la etapa del procedimiento 200 y a la aportación de la información de contexto del controlador K en otro mensaje en la etapa del procedimiento 201, pueden proporcionarse ambos mensajes conjuntamente en una etapa del procedimiento del dispositivo de enlace del controlador 41. Por ejemplo pueden transmitirse el mensaje de challenge C y la información de contexto del controlador K en un mensaje común o un fichero común.

Alternativamente pueden proporcionarse el mensaje de challenge C y la información de contexto del controlador K mediante otra entidad, por ejemplo un dispositivo de distribución de claves (Key Distribution) o bien un centro de distribución de claves (Key Distribution Center) KDC.

En una etapa siguiente del procedimiento 202 se realiza un cálculo de una función Context-Binding (función de enlace de contexto) CB(K; C) = C'. La función Context-Binding CB sirve para enlazar la información de contexto del controlador K con el mensaje challenge C para generar el mensaje challenge modificado C'. La etapa del procedimiento 202 pueden presentar otras etapas subordinadas, como por ejemplo la elección de la función Context-Binding CB() o bien la aportación de la función Context-Binding CB() mediante lectura desde una memoria de datos. El mensaje challenge modificado C' generado puede denominarse también alternativamente challenge C' específico del contexto.

En una etapa del procedimiento 203 que va a continuación se realiza la transmisión del mensaje challenge modificado C' al aparato 42.

En una etapa del procedimiento 204 que va a continuación se realiza un cálculo del mensaje response R en función del mensaje challenge modificado C' aportado. El cálculo del mensaje response R se realiza con una función de derivación de clave f(C') = R. La aportación del mensaje response R puede incluir otras etapas subordinadas, como por ejemplo la elección de la función de derivación de claves f(). Además puede realizarse el cálculo del mensaje de respuesta utilizando una clave criptográfica.

En una etapa del procedimiento 205 que va a continuación se realiza la transmisión del mensaje response R desde el aparato 42 al dispositivo de enlace del controlador 41. En una etapa del procedimiento 206 que va a continuación transmite el dispositivo de enlace del controlador 41 el mensaje response R al dispositivo de prueba 40. Se realiza así una retransmisión del mensaje response R desde el aparato 42 al dispositivo de prueba 40. En una etapa del procedimiento alternativa a las etapas del procedimiento 205 y 206 se transmite el mensaje response R directamente desde el aparato 42 al dispositivo de prueba 40.

En una etapa del procedimiento 207 que va a continuación se realiza el cálculo de las informaciones Context-Binding CB(K; C) = C'. Para ello puede ser necesario que el dispositivo de enlace del controlador 41 transmita la información

de contexto del controlador K al dispositivo de prueba 40. La información de contexto del controlador K aportada sirve como parámetro de entrada de la función Context-Binding CB(K; C). Con ello se calcula en la etapa del procedimiento 207, análogamente a en la etapa del procedimiento 202, la función Context-Binding para la información de contexto del controlador K y el mensaje challenge C.

En una etapa del procedimiento 208 que va a continuación se realiza una verificación del mensaje response R proporcionado en la etapa del procedimiento 206 y del mensaje de consulta modificado C' calculado en la etapa del procedimiento 207. En consecuencia se comprueba en la etapa del procedimiento 208 si el mensaje response R proporcionado en la etapa del procedimiento 206 representa la respuesta esperada al mensaje de consulta o mensaje challenge C proporcionado en la etapa del procedimiento 200. La función de verificación que encuentra aplicación en la etapa del procedimiento 208 puede denominarse por ejemplo Response Verification-Funktion (función de verificación de respuesta) RV(R; C'). Como valor de devolución aporta esta función Response-Verification RV() un Valor de Bool, que indica si el mensaje response R proporcionado en la etapa del procedimiento 206 es la respuesta esperada al mensaje challenge modificado C'. Se comprueba así en la etapa del procedimiento 208, utilizando los parámetros ya empleados, la identidad del aparato 42.

Las etapas del procedimiento descritas pueden realizarse iterativamente y/o en otra secuencia.

La figura 8 describe un procedimiento para modificar un mensaje de consulta C en función de una información de contexto del controlador K, en particular para operar un dispositivo de enlace del controlador 41 según la figura 5, con las siguientes etapas:

En una etapa del procedimiento 300 se aporta la información de contexto del controlador K a una unidad de enlace del controlador 41. A continuación se aporta 301 el mensaje de consulta C a la unidad de enlace del controlador 41. Además se realiza un cálculo de un mensaje de consulta modificado C' en función de la información de contexto del controlador K proporcionada y del mensaje de consulta C proporcionado.

Las etapas del procedimiento antes descritas pueden realizarse iterativamente y/o en otra secuencia.

La figura 9 describe un diagrama secuencial detallado de una forma de realización del procedimiento para autentificar con fiabilidad un aparato 42. Aquí comunica un servidor 93 con un aparato 91 mediante el módulo M2M 92. El módulo M2M 92 puede existir por ejemplo como un componente típico de la red.

El aparato 91 establece mediante el módulo M2M 92 un enlace SSL con el servidor 93. Aquí no se han representado los distintos mensajes de una estructura de enlace SSL. En el presente ejemplo de ejecución se autentifican el servidor 93 y el aparato 91 en un proceso de autentificación Auth. En una etapa del procedimiento S10 se memoriza el servidor 10. A continuación envía el servidor 93 un get_device_cert GDC al aparato 91. Este mensaje get_device_cert GDC es transmitido por el aparato 91 a una unidad de autentificación de aparatos 90. Esta unidad de autentificación de aparatos 90 transmite un Cert al aparato 91, que retransmite el mensaje Cert al servidor 93. En una etapa del procedimiento S11 se realiza un ajuste de un mensaje de consulta mediante el servidor 93. El servidor 93 origina una llamada al método correspondiente a un método de autentificación AuthD(c).

En una etapa del procedimiento S12 que va a continuación, se deduce el mensaje de consulta C-Bound. Esto puede realizarse por ejemplo mediante la siguiente instrucción:

Derive Challenge C-Bound: = KDF(C, Server_ID)

El mensaje C-Bound calculado es transmitido por el aparato 91 a la unidad de autentificación de aparatos 90. Esta unidad de identificación de aparatos 90 transmite a continuación un mensaje de respuesta Res al aparato 91. El aparato 91 genera a continuación una llamada al método AuthD(res).

En otra etapa del procedimiento S13 se realiza una nueva deducción del mensaje de consulta C-Bound.

Así se crea en el presente ejemplo de ejecución el mensaje de consulta C-Bound en función de un Server_ID del servidor 93. Así se crea en la etapa del procedimiento S12 un mensaje de consulta modificado según un mensaje de consulta aportado por el servidor 93 y un Server_ID del servidor 93.

Las etapas del procedimiento descritas pueden realizarse iterativamente y/o en otra secuencia.

La figura 10 muestra un diagrama secuencial detallado de un procedimiento para autentificar con fiabilidad un aparato 42 con una autentificación mediante una tercera entidad digna de confianza.

En el presente ejemplo de realización se añade al procedimiento de acuerdo con la invención, tal como se ha descrito en la figura 9, otra entidad adicional, que es un dispositivo Key-Distribution-Center (centro de distribución de claves) 94. Así se realiza una autentificación Server Side (del lado del servidor) SSL entre el aparato 91 y el servidor 93 mediante un certificado del servidor, así como una autentificación del aparato mediante un token del servidor KDC 94.

En el presente ejemplo de realización se realiza una autentificación, así como una consulta de una autorización y consulta de un mensaje de consulta según la flecha de doble sentido 95 representada en la presente figura 10.

En una etapa del procedimiento S20 se crea un mensaje de consulta C_Bound mediante un servicio de distribución de claves 94, denominado también Key Distribution Center 94.

En una siguiente etapa del procedimiento S21 se memoriza un Server_ID mediante el aparato 91. A continuación se realiza un envío de un mensaje de token con una información de autorización y el mensaje de consulta C_Bound calculado en la etapa del procedimiento S20 según el intercambio de mensajes 96 representado en la presente figura. El aparato 91 consulta a continuación en el servidor mediante el mensaje de consulta C_Bound calculado en la etapa del procedimiento S20 mediante un intercambio de mensajes 97 sobre un servicio. El servidor 93 envía a continuación un mensaje de autentificación AuthDev al aparato 91. En consecuencia dispone el aparato 91 tanto del mensaje de consulta C_Bound como también del Server_ID.

En una siguiente etapa del procedimiento S22 se realiza el enlace de la información de contexto del controlador K o bien Server_ID con el mensaje de consulta C_Bound. Esto se realiza en el presente ejemplo de ejecución mediante el aparato 91. Una posible implementación de este enlace se realiza por ejemplo mediante el siguiente texto-fuente:

Derive Challenge C-Bound: = KDF(C_Bound, Server_ID).

El mensaje CBound calculado en la etapa del procedimiento S22 se transmite a continuación a una unidad de autentificación de aparatos (device) 90. Esta unidad de autentificación de aparatos calcula a continuación un mensaje de respuesta Res y lo transmite al aparato 91. El aparato 91 provoca a continuación la ejecución de un método de autentificación con el parámetro de entrada Res.

En consecuencia se realiza en una etapa del procedimiento S23 una segunda deducción del mensaje de consulta C_Bound mediante el servidor 93. Esta segunda deducción puede implementarse por ejemplo mediante la siguiente instrucción:

Device Challenge C-Bound: = KDF(C_Bound, Server_ID).

En otra etapa del procedimiento S24 se realiza la verificación del mensaje de respuesta Re transmitido mediante el servidor 93.

En consecuencia se realizó en el presente ejemplo de ejecución una autentificación del aparato 91 mediante una información de contexto del controlador K, denominado también Server_ID en el presente ejemplo de realización. Para ello se enlazó el mensaje de consulta C_Bound mediante el Server_ID con un mensaje de consulta modificado C', denominado también C_Bound en el presente ejemplo de realización.

En comparación con el ejemplo de realización descrito en la figura 9, se realizó en consecuencia en el ejemplo de realización descrito en la figura 10 una autentificación por medio de una tercera entidad digna de confianza, que es el dispositivo Key Distribution Center.

Las etapas del procedimiento antes descritas pueden realizarse iterativamente y/o en otra secuencia.

REIVINDICACIONES

1. Dispositivo de enlace del controlador (41) para modificar un mensaje de consulta (C) en función de una información de contexto del controlador (K) con:
   - una interfaz de información de contexto del controlador (41B) para recibir la información de contexto del controlador (K) de una unidad de aportación de la información de contexto del controlador (40A) de un dispositivo de prueba (40) y para proporcionar la información de contexto del controlador (K) a una unidad de enlace del controlador (41A);
   - una interfaz de mensajes de consulta (41C) para recibir el mensaje de consulta (C) de una unidad de aportación de mensajes de consulta (40B) del dispositivo de prueba (40) y para proporcionar el mensaje de consulta (C) a la unidad de enlace del controlador (41A); y
   - la unidad de enlace del controlador (41A) que calcula un mensaje de consulta modificado (C') mediante una función Context-Binding en función de la información de contexto del controlador (K) proporcionada y del mensaje de consulta (C) proporcionado para la transmisión a un aparato (42) a autentificar mediante el dispositivo de prueba (40),

   enlazando el dispositivo de enlace del controlador (41) el mensaje de consulta (C) recibido mediante la información de contexto del controlador (K) al dispositivo de prueba (40),
   pudiendo comprobarse la autenticidad del aparato (42) en base a un mensaje response (R) aportado por el aparato (42) al mensaje de consulta modificado (C') mediante el dispositivo de prueba (40).

2. Sistema para la autentificación fiable de un aparato (42) con:
   - un dispositivo de prueba (40), que en función de un mensaje de respuesta (R) verifica una identidad del aparato (42),
   - un dispositivo de enlace del controlador (41) de acuerdo con la reivindicación 1,
   - el aparato (42), calculando el aparato (42) el mensaje de respuesta (R) en función del mensaje de consulta modificado (C').

3. Sistema de acuerdo con la reivindicación 2,
   en el que la información de contexto del controlador (K) se crea en dependencia de al menos una característica del dispositivo de prueba (40).

4. Sistema de acuerdo con la reivindicación 3,
   en el que el dispositivo de prueba (40) presenta una característica de identidad, una dirección de IP, un nombre de ordenador, una dirección MAC, un certificado, una clave de sesión, una clave y/o un token de autentificación.

5. Sistema de acuerdo con una de las reivindicaciones 2 a 4,
   en el que el dispositivo de gestión de claves KDC (94) proporciona la información de contexto del controlador (K) y/o el mensaje de consulta (C).

6. Sistema de acuerdo con una de las reivindicaciones 2 a 5,
   en el que el dispositivo de enlace del controlador (41) presenta una primera unidad de modificación de consultas (41A), que calcula el mensaje de consulta modificado (C') según una función de derivación de claves en dependencia de la información de contexto del controlador (K) y del mensaje de consulta (C).

7. Sistema de acuerdo con la reivindicación 6,
   en el que el dispositivo de prueba (40) verifica el mensaje de respuesta (R) mediante una segunda unidad de modificación de consultas (40C) y una unidad de verificación de respuesta (40D), calculando la segunda unidad de modificación de consultas (40C) el mensaje de consulta modificado (C') según la función de derivación de claves y verificando la unidad de verificación de respuesta (40D) el mensaje de respuesta (R) en función del mensaje de consulta modificado (C') calculado.

8. Sistema de acuerdo con la reivindicación 6 ó 7,
   en el que una unidad de elección elige la función de derivación de claves a partir de un conjunto de funciones de derivación de claves memorizadas en una memoria de datos y proporciona la función de derivación de claves elegida al menos a una de las unidades de modificación de consultas (41A; 40C)

9. Sistema de acuerdo con la reivindicación 8,
   en el que el conjunto memorizado de funciones de derivación de claves presenta MD5, SHA-1, SHA-256, SHA-512, HMAC y CRC32.

10. Sistema de acuerdo con una de las reivindicaciones 2 a 9,
    en el que el aparato (42) transmite el mensaje de respuesta (R) calculado al dispositivo de enlace del controlador (41) y el dispositivo de enlace del controlador (41) transmite el mensaje de respuesta (R) calculado al dispositivo de prueba (40).:

11. Sistema de acuerdo con una de las reivindicaciones 2 a 9,
    en el que el aparato (42) transmite el mensaje de respuesta (R) calculado al dispositivo de prueba (40).

12. Producto de programa de ordenador para operar un sistema de acuerdo con una de las reivindicaciones 2 a 11 y/o para operar un dispositivo de enlace del controlador (41) según la reivindicación 1.

13. Memoria de datos, que memoriza el producto de programa de ordenador según la reivindicación 12.

14. Procedimiento para modificar un mensaje de consulta (C) en función de una información de contexto del controlador (K) en el que un dispositivo de enlace del controlador (41) ejecuta las siguientes etapas:
- recepción de la información de contexto del controlador (K) mediante una interfaz de información de contexto del controlador (41B) de una unidad de aportación de información de contexto del controlador (40A) de un dispositivo de prueba (40) y aportación de la información de contexto del controlador (K) a una unidad de enlace del controlador (41A);
- recepción del mensaje de consulta (C) mediante una interfaz de mensajes de consulta (41C) de una unidad de aportación de mensajes de consulta (40B) del dispositivo de prueba (40) y aportación del mensaje de consulta (C) a la unidad de enlace del controlador (41A); y
- cálculo de un mensaje de consulta modificado (C'), estando prevista la unidad de enlace del controlador (41A) en el dispositivo de enlace del controlador (41) con una función Context-Binding y mediante la función Context-Binding calcula el mensaje de consulta modificado (C') en función de de la información de contexto del controlador (K) proporcionada y del mensaje de consulta (C) proporcionado y lo transmite a un aparato (42) a autentificar mediante el dispositivo de prueba (40), enlazando la función Context-Binding el mensaje de consulta (C) recibido mediante la información de contexto del controlador (K) al dispositivo de prueba (40),

pudiendo comprobarse la autenticidad del aparato (42) en base a un mensaje response (R) aportado por el aparato (42) al mensaje de consulta modificado (C') mediante el dispositivo de prueba (40).

FIG 1

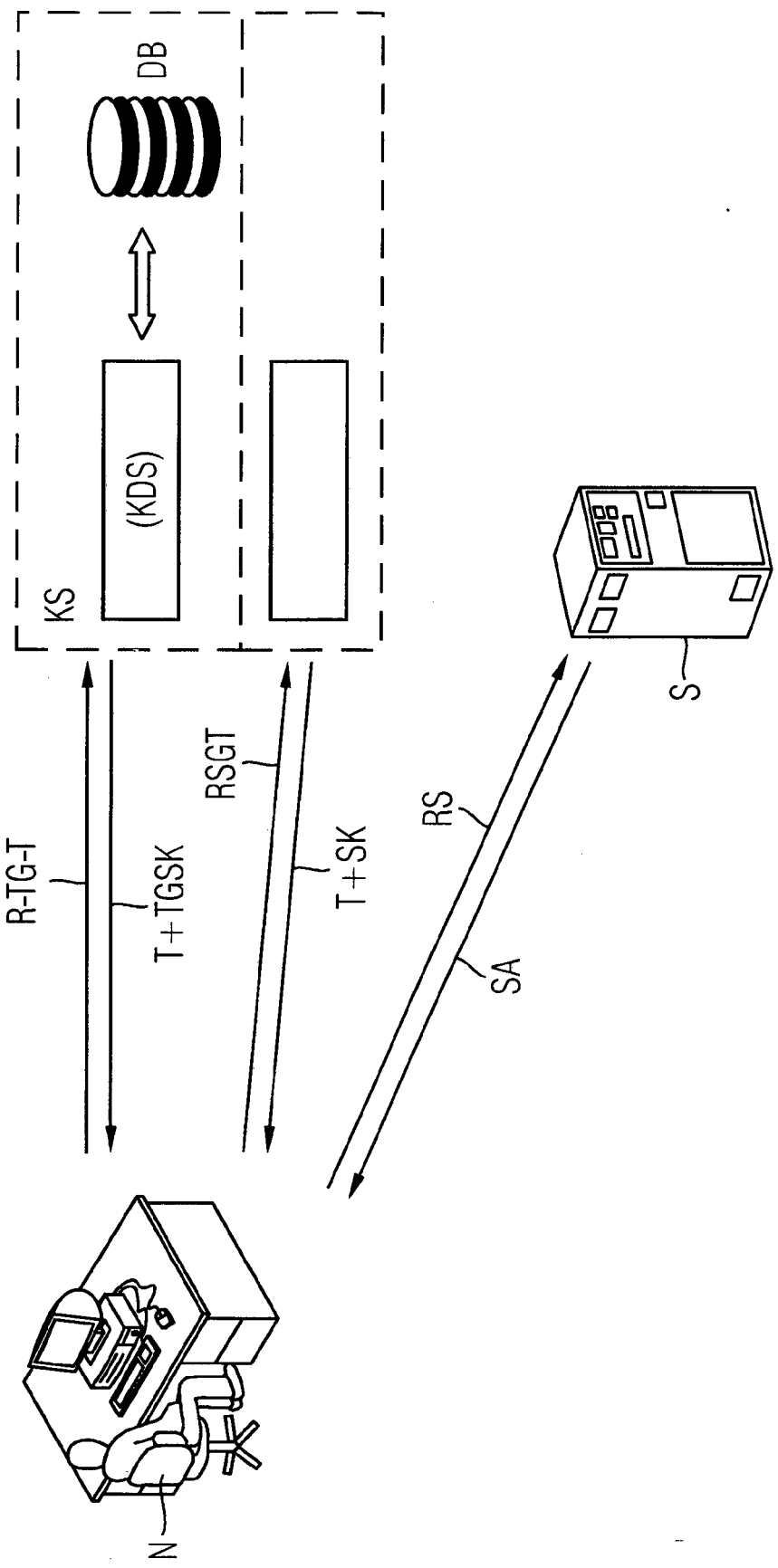


FIG 2

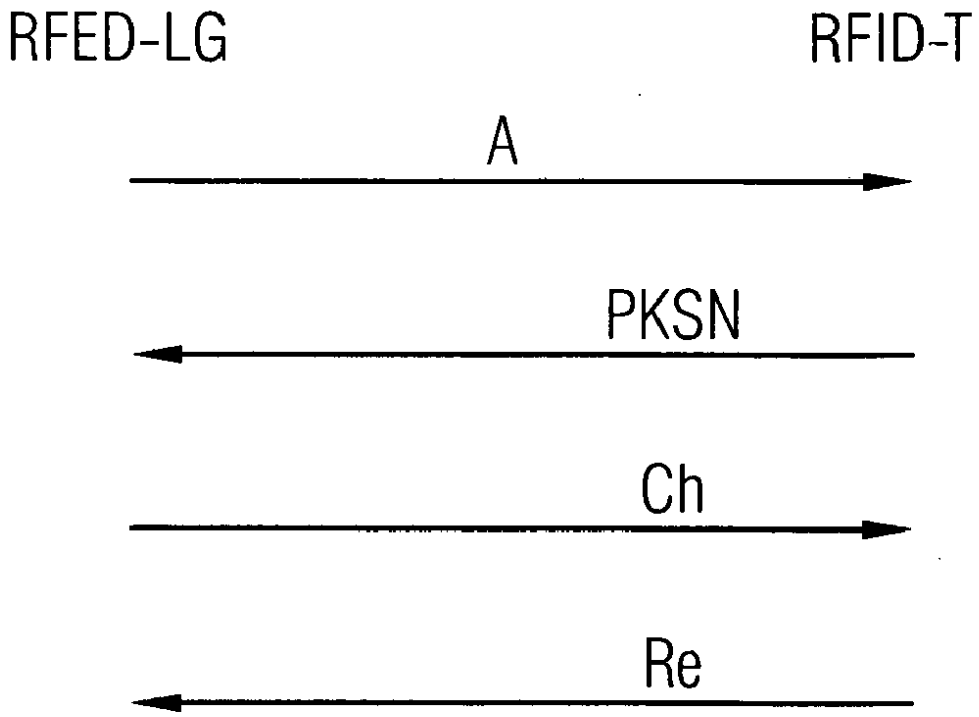


FIG 3

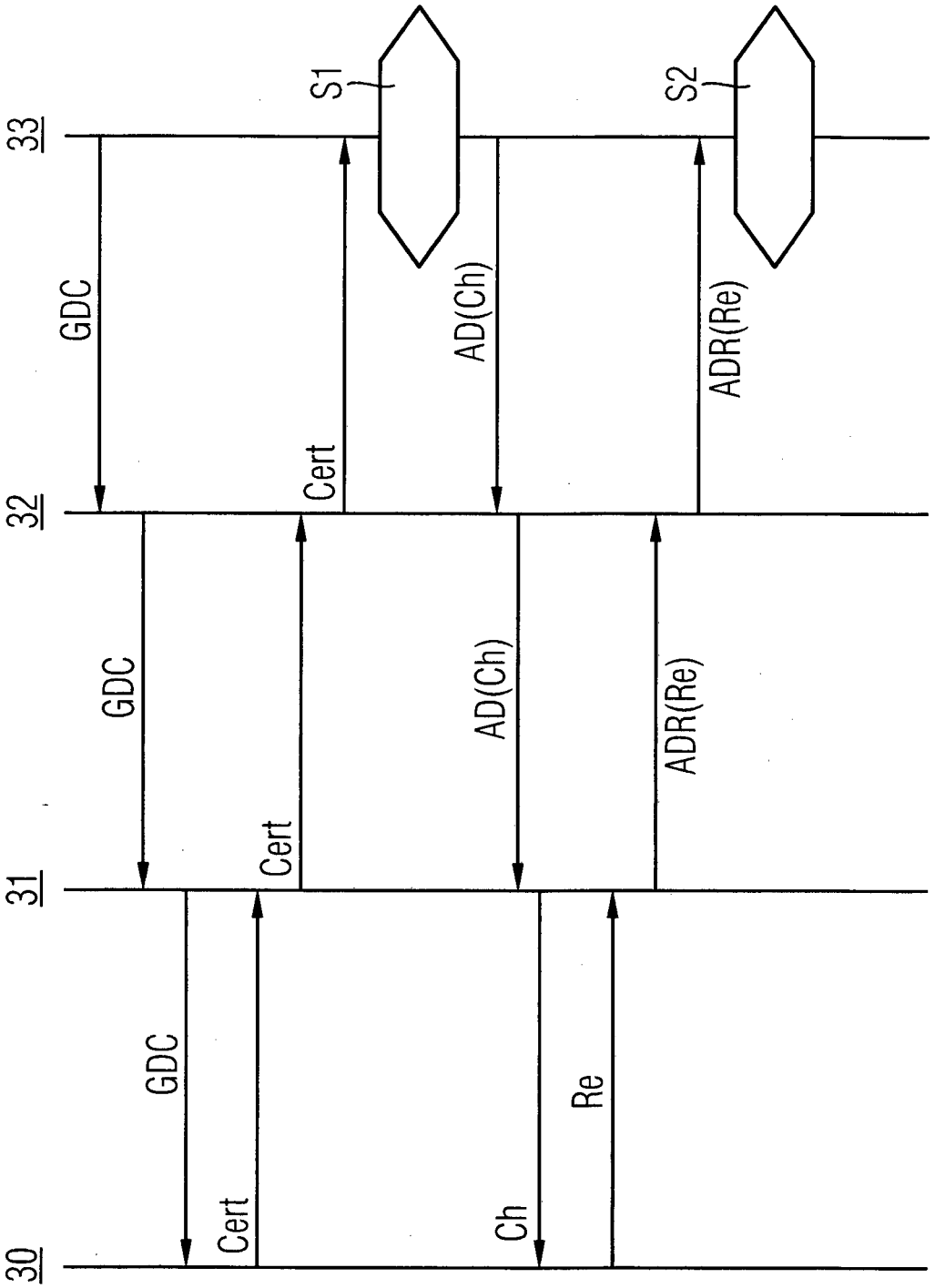

33
32
31
30
S1
S2
GDC
Cert
AD(Ch)
ADR(Re)
GDC
Cert
AD(Ch)
ADR(Re)
GDC
Cert
Ch
Re

FIG 4

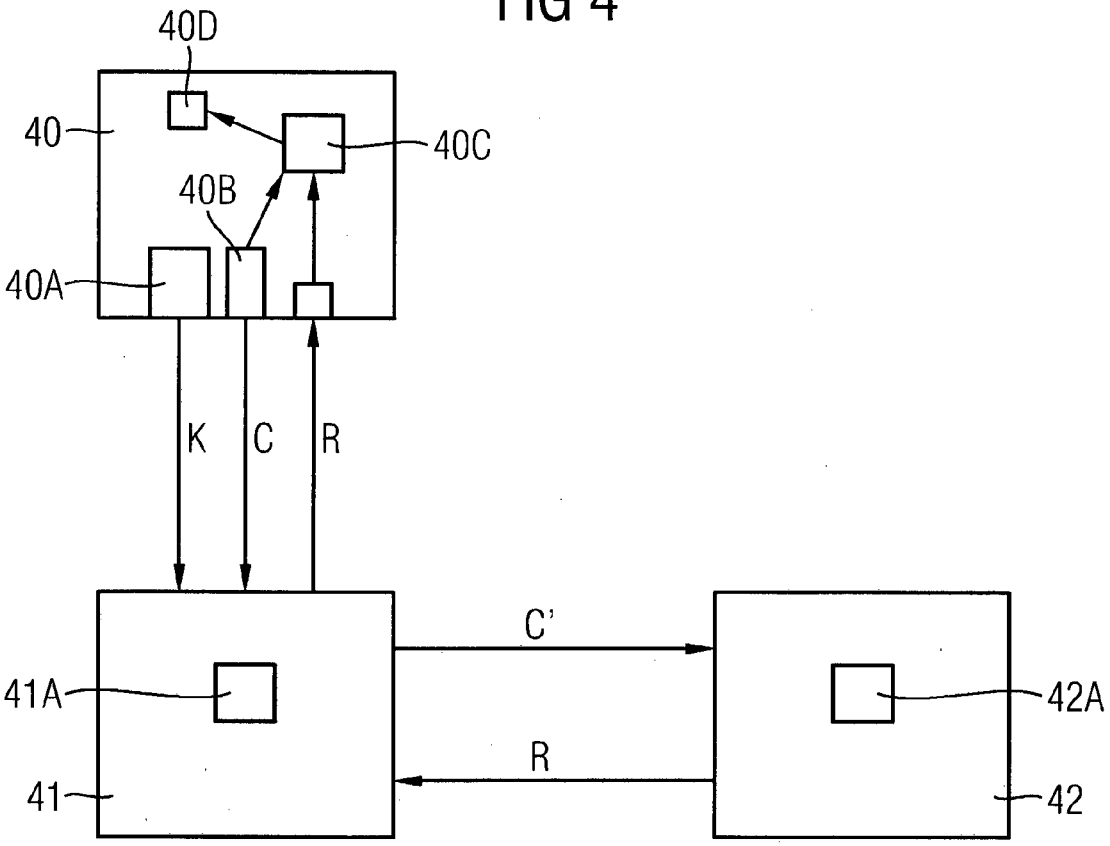


FIG 5

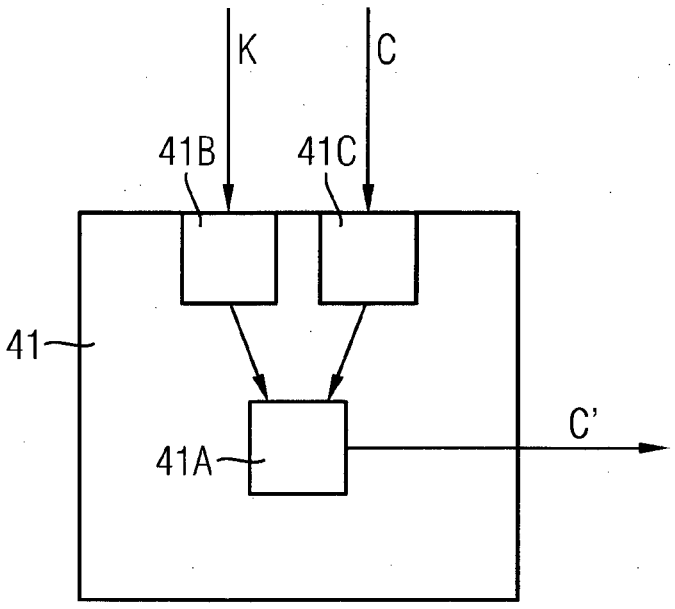


FIG 6

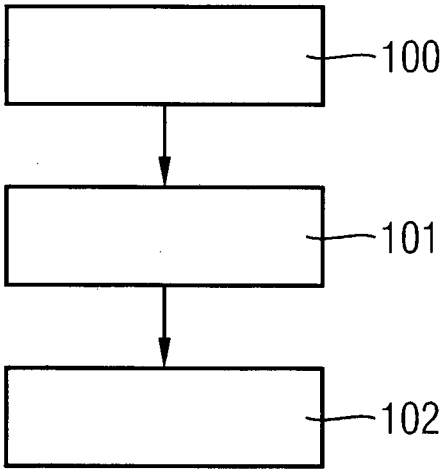


FIG 7

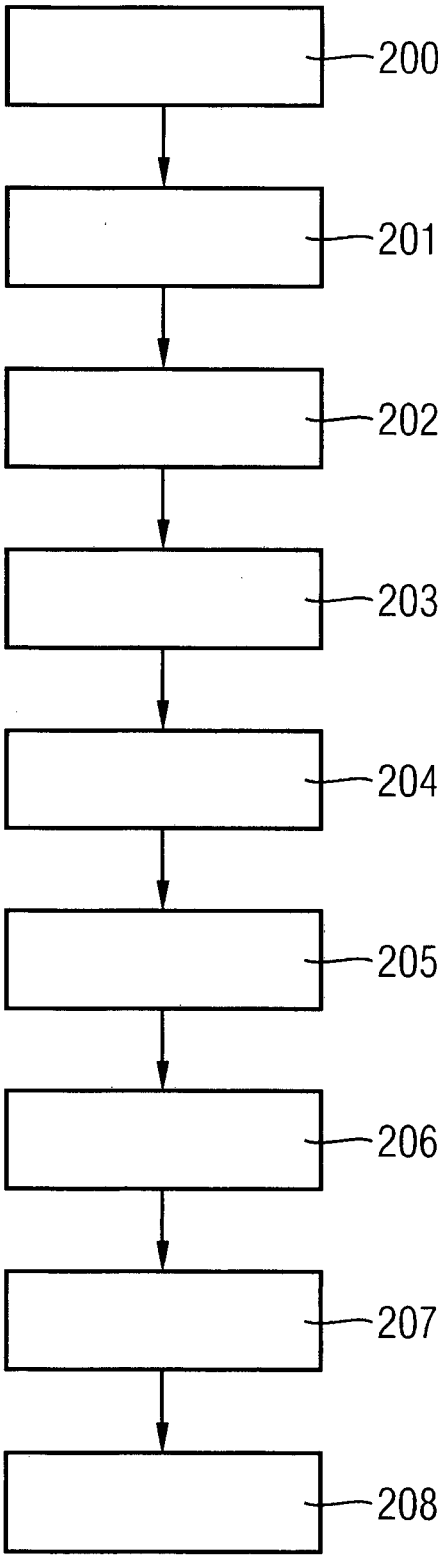


FIG 8

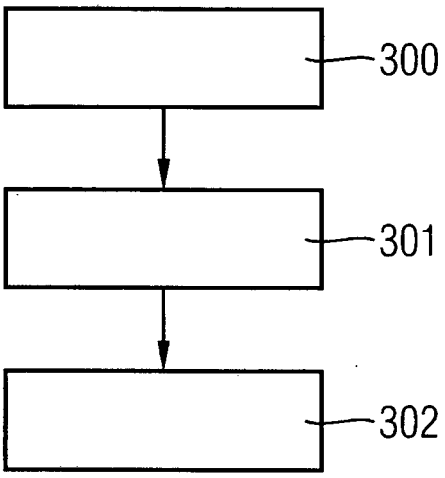


FIG 9

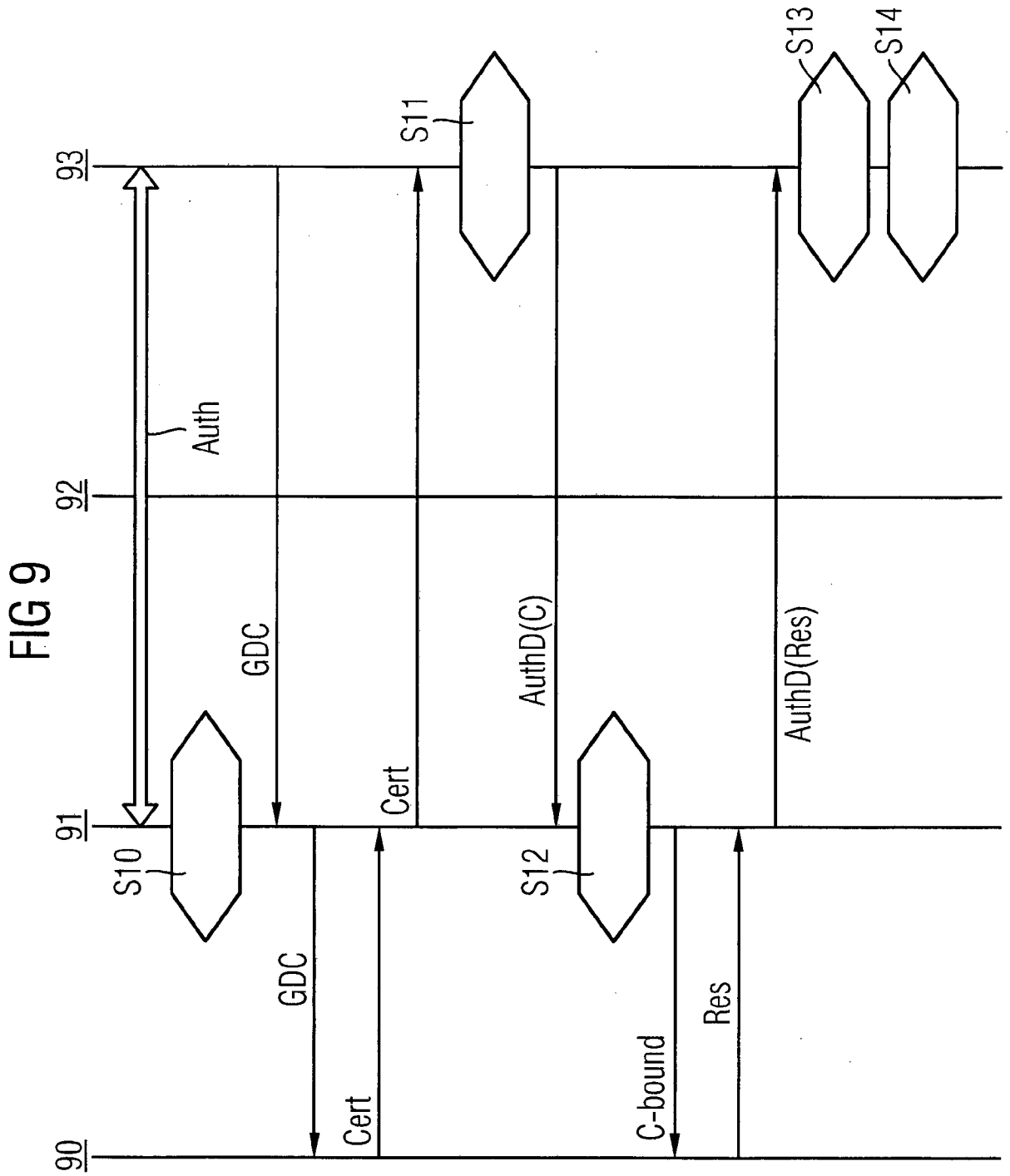
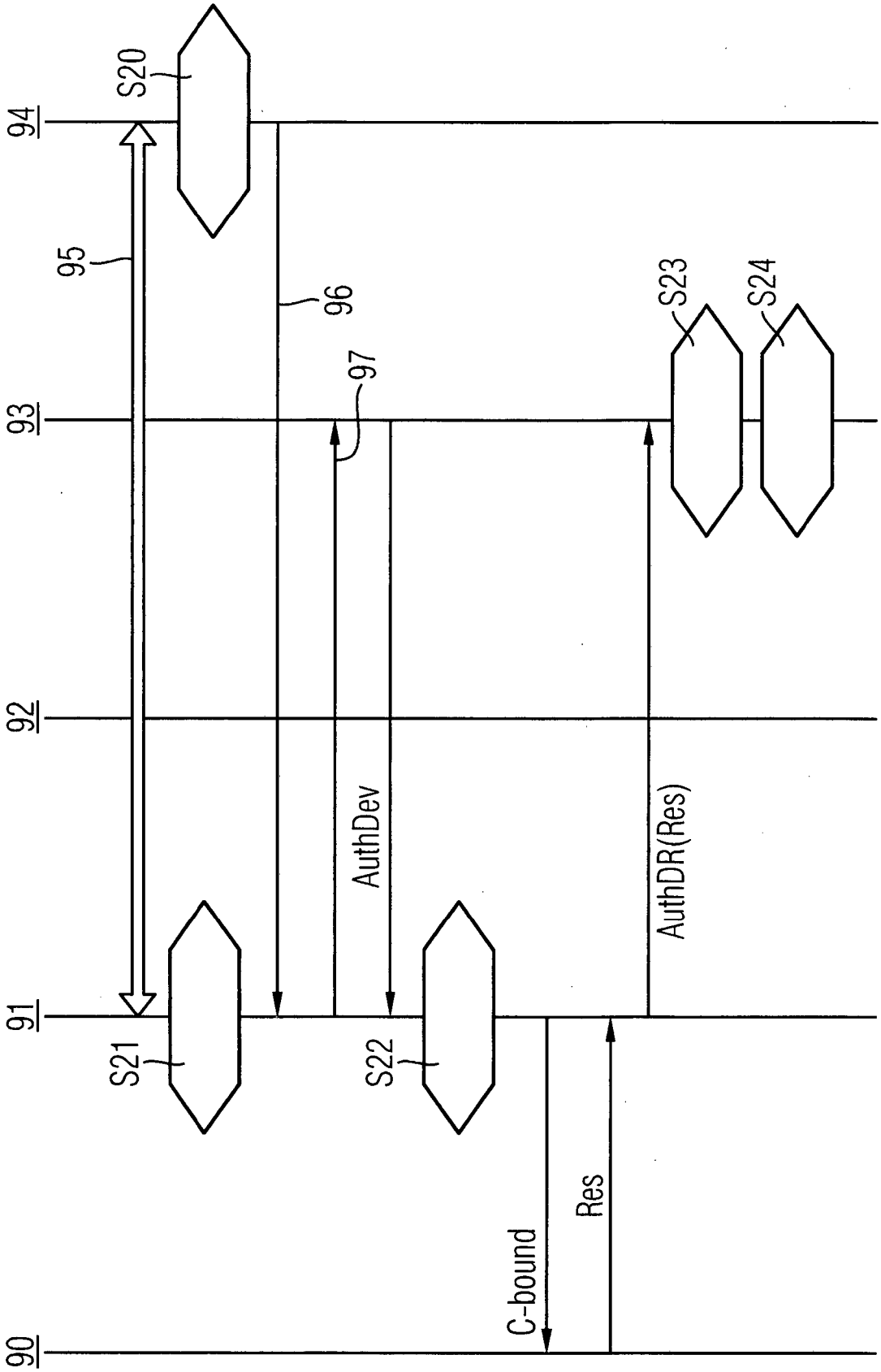

93
92
91
90
Auth
GDC
Cert
S10
S11
AuthD(C)
S12
S13
S14
AuthD(Res)
GDC
Cert
C-bound
Res

FIG 10


94
95
96
97
93
92
91
90
S20
S21
S22
S23
S24
AuthDev
AuthDR(Res)
C-bound
Res