(19) OFICINA ESPAÑOLA DE PATENTES Y MARCAS

ESPAÑA

(11) Número de publicación: **2 806 799**

(51) Int. CI.:

H04L 29/06 (2006.01)

(12) TRADUCCIÓN DE PATENTE EUROPEA T3

(96) Fecha de presentación y número de la solicitud europea: **09.08.2017 E 17185562 (0)**

(97) Fecha y número de publicación de la concesión europea: **06.05.2020 EP 3442193**

(54) Título: **Procedimiento para establecer un canal de comunicaciones seguro entre un primer y un segundo dispositivo de red**

(45) Fecha de publicación y mención en BOPI de la traducción de la patente:
18.02.2021

(73) Titular/es:

SIEMENS MOBILITY GMBH (100.0%)
Otto-Hahn-Ring 6
81739 München, DE

(72) Inventor/es:

FALK, RAINER y
FRIES, STEFFEN

(74) Agente/Representante:

CARVAJAL Y URQUIJO, Isabel

DESCRIPCIÓN

Procedimiento para establecer un canal de comunicaciones seguro entre un primer y un segundo dispositivo de red

La presente invención hace referencia a un procedimiento para establecer un canal de comunicaciones seguro para el intercambio de datos entre un primer y un segundo dispositivo de red, mediante un protocolo seguro.

Para que los datos puedan intercambiarse de forma segura entre un primer y un segundo dispositivo de red, como por ejemplo aparatos de Internet de las cosas (IdD), puede ser necesario configurar un canal de comunicaciones seguro entre el primer y el segundo dispositivo de red, donde el canal de comunicaciones seguro puede estar definido mediante un protocolo seguro. Para ello, los dispositivos de red pueden comprender datos de establecimiento de protocolo u opciones de protocolo, que establecen protocolos admisibles para el dispositivo de red.

Con frecuencia, los datos de establecimiento de protocolo ya se fijan durante la fabricación del dispositivo de red. El desarrollo rápido de protocolos, en particular de protocolos de seguridad, sin embargo, exige una actualización de los datos de establecimiento de protocolo en los dispositivos de red.

El documento US 2014/256286 A1 describe un procedimiento para la selección de protocolo inteligente, para establecer de modo más eficiente conexiones de red seguras entre un dispositivo móvil y un recurso seguro en posiciones conocidas.

El documento US 2013/227272 A1 describe una técnica que posibilita a un dispositivo de cliente almacenar una información sobre si varios dispositivos anfitriones respaldan un protocolo de seguridad determinado.

El documento EP 1 501 256 A2 describe además un dispositivo de negociación de protocolo que posibilita a un ordenador u otro nodo, que se encuentra por fuera de un área segura, negociar un protocolo de seguridad con un servidor o con otro nodo dentro del área segura.

Considerando estos antecedentes, el objeto de la presente invención consiste en crear un procedimiento mejorado para establecer un canal de comunicaciones seguro para el intercambio de datos entre un primer y un segundo dispositivo de red, mediante un protocolo seguro.

Conforme a ello se propone un procedimiento para establecer un canal de comunicaciones seguro para el intercambio de datos entre un primer y un segundo dispositivo de red, mediante un protocolo seguro, según la reivindicación 1 independiente.

En las reivindicaciones dependientes se indican otras variantes y aspectos.

La figura 1 muestra un primer ejemplo de una red.

La figura 2 muestra un procedimiento para establecer un canal de comunicaciones seguro entre un primer y un segundo dispositivo de red, según una primera forma de ejecución.

La figura 3 muestra un procedimiento para establecer un canal de comunicaciones seguro entre un primer y un segundo dispositivo de red según una segunda forma de ejecución.

La figura 4 muestra un segundo ejemplo de una red.

En las figuras, los elementos idénticos o que presentan la misma función, en tanto no se indique otra cosa, han sido provistos de los mismos símbolos de referencia.

La figura 1 muestra un primer ejemplo de una red 10. La red 10 comprende un primer dispositivo de red 1, un segundo dispositivo de red 2 y un dispositivo emisor 5.

El primer dispositivo de red 1 es un cliente que accede al segundo dispositivo de red 2, donde el segundo dispositivo de red 2 es un servidor.

Para una transmisión de datos segura entre el cliente 1 y el servidor 2, entre los mismos se establece un canal de comunicaciones 3. El establecimiento del canal de comunicaciones 3 tiene lugar mediante el procedimiento descrito en la figura 2.

A continuación, mediante las figuras 1 y 2, se describe cómo se establece un canal de comunicaciones seguro entre el primer y el segundo dispositivo de red, según una primera forma de ejecución.

En un paso de preparación S0 se preparan el cliente 1, el servidor 2 y el dispositivo emisor 5.

En un paso S1, datos de seguridad son creados mediante el dispositivo emisor 5. El dispositivo emisor 5 genera los datos de seguridad como un JSON Web Token. Los datos de seguridad creados reciben datos de establecimiento de protocolo para el servidor 2. Los datos de establecimiento de protocolo, entre otras cosas, establecen que entre el cliente 1 y el servidor 2 debe estar presente un protocolo 4 seguro en la versión TLS TLS1.2 Para proteger los datos de seguridad, los mismos se firman con una firma digital, mediante el dispositivo emisor 5.

En un paso S2, el dispositivo emisor 5 transmite los datos de seguridad creados al cliente 1, mediante una red 6. El cliente 1 retransmite los datos de seguridad al servidor 2, en un paso S3.

La transmisión de los datos de seguridad, desde el cliente 1 hacia el servidor 2, tiene lugar en un protocolo TLS-Handshake. El TLS-Handshake permite además al servidor 2 autenticarse en el cliente 1. Para que los datos de seguridad del TLS-Handshake puedan transmitirse al servidor 2, un protocolo TLS habitual y un protocolo TLS-Handshake habitual deben ser ampliados.

Una ampliación de un protocolo TLS según RFC 6066 para la transmisión de los datos de seguridad, para la implementación en lenguajes de programación difundidos, como C o C++, puede comprender la siguiente definición:

```
enum {
     ECB (0), OFB (1), CBC (2), GCM (3), GMAC (4), OCB(5),
EAX (6), CWC (7), (255)
} AlgorithmMode

struct {
     bool              sessionResumption,
     bool              sessionRenegotiation,
     bool              compression,
     bool              anonymous,
     bool              unilateral,
     bool              mutual,
     bool              PSK,
     bool              certificates
} ProtocolFeatures

struct {
     ByteString        fingerprint-App-1,
     ByteString        fingerprint-App-2,
     ByteString        fingerprint-App-3,
     ByteString        fingerprint-App-4,
     ByteString        fingerprint-App-5
} PermittedApps

struct {
     int               port-App-1,
```

```
        int                 port-App-2,
        int                 port-App-3,
        int                 port-App-4,
        int                 port-App-5
    } PermittedPorts

    struct {
        int                 oidSecPol,
        ByteString          authAlgorithm   // algorithm OID,
        ByteString          intAlgorithm    // algorithm OID,
        AlgorithmMode       intMode,
        ByteString          encAlgorithm    // algorithm OID,
        AlgorithmMode       encMode,
        int                 keyLengthMin,
        int                 keyAgeMin,
        int                 keyAgeMax,
        ProtocolFeatures    protFeat,
        time                validityStart,
        time                validityEnd,
        PermittedApps       pApp,
        PermittedPorts      pPort,
        Signature           authorization   // signature of poli-
                            cy issuer
    } SecPol
```

Se amplían además los tipos de mensajes del protocolo TLS-Handshake, para poder transmitir datos de seguridad. Para ello, los tipos de mensajes del protocolo TLS-Handshake se amplían en un tipo de mensajes de pñitica de sesión "session_policy", del siguiente modo:

```
enum {
    hello_request(0), client_hello(1), server_hello(2),
    certificate(11), server_key_exchange (12),
    certificate_request(13), server_hello_done(14),
    certificate_verify(15), client_key_exchange(16),
    finished(20), session_policy (21), (255)
} HandshakeType;
struct {
    HandshakeType msg_type; /* handshake type */
    uint24 length; /* bytes in message */
    select (HandshakeType) {
           case hello_request: HelloRequest;
           case client_hello: ClientHello;
           case server_hello: ServerHello;
           case certificate: Certificate;
```

```
            case server_key_exchange: ServerKeyExchange;
            case certificate_request: CertificateRequest;
            case server_hello_done: ServerHelloDone;
            case certificate_verify: CertificateVerify;
            case client_key_exchange: ClientKeyExchange;
            case finished: Finished;
            case session_policy: SecPol;
        } body;
    } Handshake;
```

La ampliación descrita posibilita una transmisión de los datos de seguridad como token, en el marco del TLS Handshake, entre el cliente 1 y el servidor 2.

De manera opcional, el servidor 2 controla la firma digital de los datos de seguridad recibidos. En el caso de que éstos sean válidos, los datos de establecimiento de protocolo contenidos en los datos de seguridad se utilizan para establecer el protocolo 4 seguro, en un paso S4. El protocolo 4 seguro se determina de tal modo mediante el servidor 2, que el mismo corresponde a las condiciones previas de los datos de establecimiento de protocolo recibidos. De este modo, según los datos de establecimiento de protocolo, el protocolo 4 seguro es un protocolo TLS1.2.

En un paso S5 se establece el canal de comunicaciones 3 seguro entre el cliente 1 y el servidor 2. Para ello se utiliza el protocolo 4 seguro, que define el canal de comunicaciones 3 seguro. Mediante el canal de comunicaciones 3 seguro, el cliente 1 y el servidor 2 pueden intercambiar datos de forma segura.

Los datos de establecimiento de protocolo, durante el TLS-Handshake, pueden transmitirse al servidor 2, debido a lo cual puede determinarse de forma dinámica el protocolo 4 seguro que define el canal de comunicaciones 3 seguro.

La figura 3 muestra un procedimiento para establecer un canal de comunicaciones seguro entre un primer y un segundo dispositivo de red, según una segunda forma de ejecución. El procedimiento representado en la figura 3 es una ampliación para el procedimiento de la figura 2. La red 10 representada en la figura 1 puede realizar el procedimiento representado en la figura 3.

Los pasos S0, S1, S2, S4 y S5 son idénticos con respecto a los pasos descritos con relación a la figura 2 y por ese motivo no se describen otra vez.

En un paso S01, en el servidor 2 se almacena una lista de admisibilidad. La lista de admisibilidad, mediante una interfaz del servidor, no representada, se transmite desde un usuario al servidor 2 y se almacena en un disco duro del servidor 2, no representado. La lista de admisibilidad contiene las URLs de todos los dispositivos emisores que tienen permitido crear datos de seguridad admisibles para el servidor 2.

Al crearse los datos de seguridad mediante el dispositivo emisor 5, en el paso S1, a los datos de seguridad se asocia una URL que indica al dispositivo emisor 5 como emisor de los datos de seguridad.

Los datos de seguridad, en el paso S2, se transmiten al cliente 1, y en un paso S3' se transmiten al servidor 2. El paso S3' se diferencia del paso S3 antes descrito en el hecho de que la transmisión de los datos de seguridad no tiene lugar mediante un TLS-Handshake, sino mediante un protocolo provisional inicial.

El protocolo provisional inicial es un protocolo HTTP que fue configurado provisionalmente entre el cliente 1 y el servidor 2, y con el cual deben verificarse los datos de establecimiento de protocolo que se encuentran presentes en los datos de seguridad.

En un paso S31, mediante el servidor 2 se verifica si el dispositivo emisor asociado a los datos de seguridad tiene permitido crear datos de seguridad admisibles según la lista de admisibilidad. El servidor 2 verifica si el dispositivo emisor asociado se encuentra presente o no en la lista de admisibilidad. En el caso de que el dispositivo emisor asociado no tenga permitido crear datos de seguridad, en un paso S34 se interrumpe el establecimiento del canal de comunicaciones seguro. En el paso S34 se emite además una señal de alarma a un usuario.

En el caso de que el dispositivo emisor asociado tenga permitido crear los datos de seguridad, en un paso S32 se verifica si el protocolo provisional inicial corresponde a las condiciones previas indicadas mediante los datos de establecimiento de protocolo, para el protocolo seguro. Por ejemplo, se verifica si el protocolo provisional inicial es un protocolo TLS1.2.

Si no se corresponde a las condiciones previas para el protocolo seguro, en un paso S35 se interrumpe la comunicación entre el cliente 1 y el servidor 2, mediante el protocolo provisional inicial.

En el caso de que se corresponda a las condiciones previas para el protocolo seguro, el protocolo provisional inicial, en un paso S33, se establece como el protocolo seguro, y el canal de comunicaciones 3 seguro se establece en el paso S5, según el protocolo seguro.

La figura 4 muestra un segundo ejemplo de una red 11. La red 11 se diferencia de la red 10 del primer ejemplo en el hecho de que el cliente 1 está conectado al servidor 2 mediante la Internet 8. A la Internet 8 están conectados también dos dispositivos de campo 7. El servidor 2 forma parte de una instalación 9, que en este caso es una instalación industrial. El servidor 2, mediante un bus 12, está conectado a otros dispositivos de campo 17a - 17c de la instalación industrial 9.

El intercambio de datos entre el cliente 1 y el servidor 2 tiene lugar mediante el canal de comunicaciones 3 seguro que, del modo antes descrito, está definido mediante el protocolo 4 seguro. Para el establecimiento del canal de comunicaciones 3 seguro se realiza el procedimiento ya descrito, de las figuras 2 ó 3.

El procedimiento de las figuras 2 ó 3, también para el establecimiento de otros canales de comunicaciones 13 seguros, puede realizarse entre el servidor 2 y los otros respectivos dispositivos de campo 17a - 17c. El servidor 2, en este caso, es el primer dispositivo de red y los respectivos dispositivos de campo 17a - 17c son los segundos dispositivos de red.

A continuación se describe cómo se realiza el procedimiento de la figura 2 para el establecimiento de otro canal de comunicaciones 13 entre el servidor 2 y el dispositivo de campo 17a. El establecimiento de otros canales de comunicaciones entre el servidor 2 y los dispositivos de campo 17b y 17c es idéntico.

En el paso S1, los otros datos de seguridad son creados mediante el dispositivo emisor 5. Los otros datos de seguridad, con los otros datos de establecimiento de protocolo, establecen otro protocolo 14 seguro entre el servidor 2 y el otro dispositivo de campo 17a.

En el paso S2, el servidor 2, por ejemplo mediante el canal de comunicaciones 3 seguro, recibe los otros datos de seguridad para el otro dispositivo de campo 17a.

En el paso S3, el servidor 2 transmite los otros datos de seguridad al otro dispositivo de campo 17a, que en el paso S4, mediante los otros datos de establecimiento de protocolo contenidos en los otros datos de seguridad, establece el otro protocolo seguro 14. En el paso S5 se establece el otro canal de comunicaciones 13 seguro entre el servidor 2 y el otro dispositivo de campo 17a, mediante el cual pueden intercambiarse datos seguros entre el servidor 2 y el otro dispositivo de campo 17a.

Aunque la presente invención fue descrita mediante ejemplos de ejecución, la misma puede modificarse de diversas formas. Por ejemplo, el primer y el segundo dispositivo de red puede ser también otros dispositivos, como dispositivos de campo, partes de robots, relés de protección o similares. Los datos de establecimiento de protocolo, por ejemplo, también pueden contener un tiempo de ejecución para el canal de comunicaciones seguro y/o datos de participantes de la comunicación. Los datos de seguridad también pueden transmitirse cifrados de forma criptográfica o pueden protegerse de cualquier modo contra manipulaciones. El protocolo seguro sólo es un protocolo TLS de forma ilustrativa, y de manera alternativa también puede ser un protocolo IPsec.

REIVINDICACIONES

1. Procedimiento para establecer un canal de comunicaciones (3) seguro para el intercambio de datos entre un primer dispositivo de red y un segundo dispositivo de red (1, 2) mediante un protocolo (4) seguro, donde el segundo dispositivo de red (2) está configurado para establecer el protocolo (4) seguro en función de datos de establecimiento de protocolo que indican condiciones previas para el protocolo (4) seguro, el cual comprende:

producción (S1) de datos de seguridad mediante un dispositivo emisor (5), donde los datos de seguridad definen los datos de establecimiento de protocolo;

firma de los datos de seguridad con una firma digital o con un código de autenticación de mensajes, mediante el dispositivo emisor (5);

transmisión (S2) de los datos de seguridad hacia el primer dispositivo de red (1), desde el dispositivo emisor (5);

transmisión (S3) de los datos de seguridad hacia el segundo dispositivo de red (2), desde el primer dispositivo de red (1);

verificación de la autenticidad de los datos de seguridad mediante el segundo dispositivo de red (2), mediante el control de la firma digital o del código de autenticación de mensajes; y

actualización de datos de establecimiento de protocolo caducados del segundo dispositivo de red (2), por medio de los datos de establecimiento de protocolo definidos mediante los datos de seguridad recibidos.

2. Procedimiento según la reivindicación 1, el cual además comprende:

establecimiento (S4) del protocolo (4) seguro mediante la utilización de los datos de establecimiento de protocolo transmitidos con los datos de seguridad al segundo dispositivo de red (2); y

establecimiento (S5) del canal de comunicaciones (3) seguro mediante el protocolo (4) seguro establecido.

3. Procedimiento según la reivindicación 1 ó 2, donde los datos de seguridad se transmiten en un protocolo de autenticación criptográfico, en particular en un protocolo TLS-Handshake.

4. Procedimiento según una de las reivindicaciones 1 a 3, donde el protocolo (4) seguro es un protocolo TLS, un protocolo DTLS, un protocolo SSH, un protocolo QUIC, un protocolo IPsec, un protocolo HTTP, un protocolo Bluetooth, un protocolo WLAN, un protocolo ZigBee, un protocolo IKE o un protocolo MACsec.

5. Procedimiento según una de las reivindicaciones 1 a 4, donde los datos de seguridad, mediante un protocolo provisional inicial, se transmiten desde el primer dispositivo de red (1) hacia el segundo dispositivo de red (2); donde el procedimiento además comprende:

verificación (S32), de si el protocolo provisional inicial corresponde a las condiciones previas indicadas mediante los datos de establecimiento de protocolo para el protocolo (4) seguro, y

establecimiento (S33) del protocolo provisional inicial como protocolo (4) seguro, en caso de que se determine que el protocolo provisional inicial corresponde a las condiciones previas para el protocolo (4) seguro.

6. Procedimiento según una de las reivindicaciones 1 a 5, donde los datos de seguridad están codificados como estructura de datos ASN.1, como estructura de datos XML, como estructura de datos JSON o como JSON Web Token.

7. Procedimiento según una de las reivindicaciones 1 a 6, donde los datos de seguridad sólo pueden descifrarse mediante el segundo dispositivo de red (2).

8. Procedimiento según una de las reivindicaciones 1 a 7, donde a los datos de seguridad está asociado un dispositivo emisor (5) que ha producido los datos de seguridad.

9. Procedimiento según la reivindicación 8, que además comprende:

almacenamiento (S01) de una lista de admisibilidad en el segundo dispositivo de red (2), que indica qué dispositivos emisores (5), de una pluralidad de dispositivos emisores, tienen permitido crear datos de seguridad admisibles para establecer el canal de comunicaciones (3) seguro;

verificación (S31), en el segundo dispositivo de red (2), de si el dispositivo emisor (5) asociado a los datos de seguridad tiene permiso para crear datos de seguridad admisibles según la lista de admisibilidad; y

establecimiento (S4) del protocolo seguro mediante la utilización de los datos de establecimiento de protocolo transmitidos con los datos de seguridad, en caso de que se determine que el dispositivo emisor (5) asociado a los datos de seguridad tiene permitido crear datos de seguridad admisibles según la lista admisibilidad.

10. Procedimiento según una de las reivindicaciones 1 a 9, donde los datos de seguridad contienen datos de establecimiento de protocolo, y/o donde los datos de seguridad contienen una dirección que indica un lugar de almacenamiento de los datos de establecimiento de protocolo.

11. Procedimiento según una de las reivindicaciones 1 a 10, donde los datos de establecimiento de protocolo contienen al menos:

datos de identificación de protocolo para identificar el protocolo (4) seguro;

datos de clave para determinar una clave que debe negociarse para el canal de comunicaciones (3) seguro;

datos de protección para determinar una protección para el canal de comunicaciones (3) seguro;

datos del tiempo de ejecución para indicar un tiempo de ejecución durante el cual el canal de comunicaciones (3) seguro puede utilizarse para el intercambio de datos entre el primer y el segundo dispositivo de red (1, 2);

datos de protocolo para definir propiedades de protocolo del protocolo (3) seguro; y/o datos de participantes de la comunicación para determinar condiciones previas para el primer y/o el segundo dispositivo de red (1, 2).

12. Procedimiento según una de las reivindicaciones 1 a 11, donde a los datos de seguridad están asociados al menos un periodo absoluto por el cual son válidos los datos de seguridad, y/o un número de canales de comunicaciones para los cuales son válidos los datos de seguridad.

FIG 1

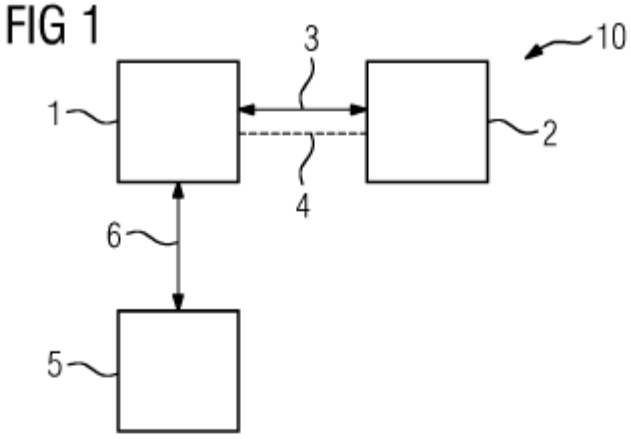

FIG 2

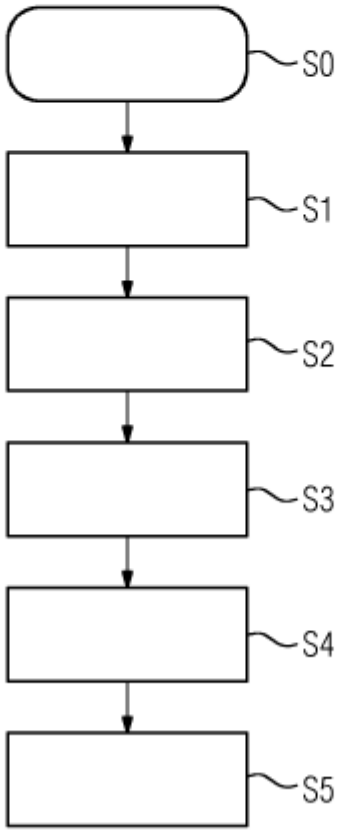

FIG 3

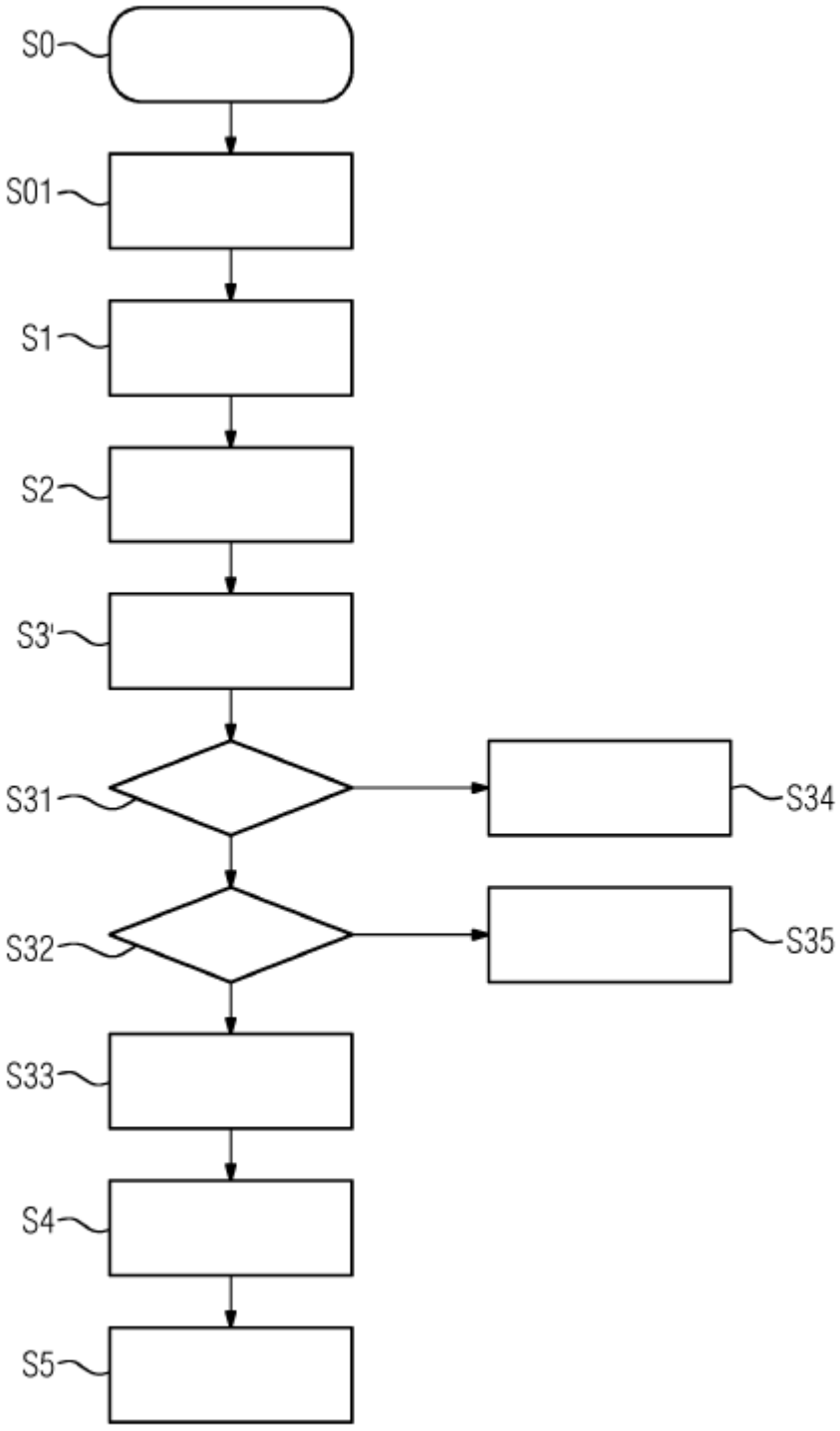

FIG 4