(19) OFICINA ESPAÑOLA DE PATENTES Y MARCAS

ESPAÑA

(11) Número de publicación: **2 628 907**

(51) Int. CI.:

H04L 29/06 (2006.01)

(12) TRADUCCIÓN DE PATENTE EUROPEA T3

(96) Fecha de presentación y número de la solicitud europea: **30.06.2015 E 15174548 (6)**

(97) Fecha y número de publicación de la concesión europea: **19.04.2017 EP 3113438**

(54) Título: **Método para la configuración de aparatos electrónicos, particularmente para la configuración de componentes de un sistema de control de acceso**

(45) Fecha de publicación y mención en BOPI de la traducción de la patente:
04.08.2017

(73) Titular/es:

SKIDATA AG (100.0%)
Untersbergstrasse 40
5083 Grödig/Salzburg, AT

(72) Inventor/es:

KEYSER, YORK

(74) Agente/Representante:

TOMAS GIL, Tesifonte Enrique

DESCRIPCIÓN

Método para la configuración de aparatos electrónicos, particularmente para la configuración de componentes de un sistema de control de acceso

[0001] La presente invención se refiere a un método para la configuración de aparatos electrónicos y particularmente para la configuración de componentes de un sistema de control de acceso para personas o vehículos.

[0002] Sistemas de control de acceso conocidos del estado de la técnica comprenden generalmente varios dispositivos de control de acceso con una unidad de lectura para la lectura de la comprobación de la validez de una autorización de acceso y un dispositivo de cierre, que es accionado por un actuador controlado por un dispositivo de control, para permitir que una persona o un vehículo entre o salga de un edificio o espacio.
Los dispositivos de control de acceso comprenden además distribuidores automáticos para las autorizaciones de acceso y/o máquinas automáticas de pago de la tasa necesaria para el uso de un sistema de control de acceso.

[0003] Del estado de la técnica se conoce, para la instalación y configuración de un componente nuevo de un sistema de este tipo, instalar en primer lugar mediante un medio de almacenamiento, por ejemplo mediante una tarjeta SD, sobre un aparato de un sistema operativo.

[0004] Este sistema operativo es generalmente un sistema operativo general, que no está adaptado al aparato por instalar. Así, la configuración IP o la definición de parámetros importantes y variables del entorno, como p.ej., direcciones del servidor, se tiene que realizar manualmente.

[0005] Del estado de la técnica se conoce también, que después de la instalación del sistema operativo general se usa un lápiz USB preconfigurado, que se lee por medio de un software preinstalado sobre el aparato por configurar (un así denominado programa de arranque). Mediante este software se descargan desde el lápiz USB los parámetros de configuración necesarios, p.ej. hora, fecha y variables del entorno, y se instalan en el sistema operativo. Después de esta fase un técnico establece mediante un protocolo de red SSH una conexión entre el aparato por configurar y otro aparato y crea una palabra clave nueva. Con ocasión de la introducción de la palabra clave nueva pueden ocurrir errores, cuando p.ej. esta no se introduce correctamente.
Además, generalmente se realiza la introducción de la palabra clave nueva de forma no codificada, lo que puede resultar en situaciones críticas de seguridad.

[0006] Para establecer una dirección IP por medio del programa de arranque, tiene que ser conocida la dirección MAC (dirección de control de acceso al medio, es decir, la dirección hardware del adaptador de red del aparato por configurar), lo que no siempre es el caso. Por tanto, un técnico se tiene que registrar en el aparato por configurar para la realización de la configuración IP a mano, cuando la dirección MAC no es conocida.
Otra parte del estado de la técnica se divulga por la solicitud de patente estadounidense US2007/118745A1.
La presente invención tiene la tarea de presentar un método para la configuración de aparatos electrónicos y especialmente para la configuración de componentes de un sistema de control de acceso para personas o vehículos, por medio de cuya realización se evitan las desventajas mencionadas anteriormente del estado de la técnica.

[0007] Esta tarea se resuelve mediante las características de la reivindicación 1.
Otras ventajas y configuraciones según la invención se deducen de las reivindicaciones secundarias.

[0008] Por consiguiente, se propone un método para la configuración de aparatos electrónicos y particularmente para la configuración de componentes de un sistema de control de acceso para personas o vehículos, en cuyo marco se usa un aparato de configuración que se puede conectar al aparato por configurar, donde la conexión puede ser por cable o inalámbrica.

[0009] El aparato de configuración es un aparato con CPU propia, medios de almacenamiento y software y comprende un así llamado entorno de ejecución seguro, es decir, una zona en el almacenamiento no volátil y/o en la CPU, a la que solo tenga acceso el software activado especialmente para ello, con lo que se pone a disposición un entorno de ejecución seguro para este software.
Tal entorno de ejecución seguro se ha desarrollado por ejemplo por la empresa ARM bajo la denominación TrustZone.

[0010] El aparato de configuración se realiza preferiblemente como lápiz USB, pero también se puede realizar como un ordenador pequeño con una alimentación eléctrica externa.

[0011] El método según la invención comprende los siguientes pasos:
Conexión del aparato de configuración con el aparato por configurar para el objetivo de la comunicación de datos de forma inalámbrica o por cable;

[0012] Realización de una autenticación recíproca;
Transmisión de una configuración prefijada al aparato por configurar, donde la configuración comprende ajustes de red y variables del entorno y donde un usuario puede vigilar el proceso mediante un dispositivo de visualización conectable con el aparato de configuración y manualmente puede efectuar cambios por medio de un dispositivo de entrada conectable con el aparato de configuración;
Transmisión mediante el entorno de ejecución seguro del aparato de configuración de una clave RSA o una clave criptográfica, que corresponde al estándar de seguridad actual, para permitir el acceso al aparato por configurar por medio de un protocolo SSH sobre el aparato por configurar y verificar la clave mediante una conexión codificada entre el aparato de configuración y el aparato por configurar;
Verificación de la palabra clave mediante una conexión cifrada y la introducción automática a continuación de la palabra clave;
Elaboración de un fichero que contiene todas las informaciones de configuración, por ejemplo, direcciones IP y MAC para la documentación del procedimiento de configuración, que se memoriza en el aparato de configuración fuera del entorno de ejecución seguro, donde este archivo no tiene información relevante en cuanto a la seguridad, como particularmente la clave RSA o una clave criptográfica, que corresponde al estándar de seguridad actual y contiene la palabra clave y sirve como referencia para procesos de configuración futuros;
Elaboración de una conexión para la comunicación de datos entre el aparato de configuración y otro ordenador, por ejemplo una agenda;
Elaboración de una conexión de red segura por medio de otro ordenador a un servidor, que puede ser por ejemplo una conexión-VPN;
Realización de una autenticación recíproca entre el aparato de configuración y el servidor;
Transmisión de la palabra clave, de la clave-RSA o de la clave criptográfica, que corresponde el estándar de seguridad actual y de otros parámetros predeterminados importantes mediante el ambiente de ejecución seguro del aparato de configuración sobre un ambiente de ejecución seguro sobre el servidor por medio de la conexión de red segura;
Verificación de la totalidad de la transmisión de la palabra clave, de la clave RSA y de los otros parámetros importantes; y
Después de la transmisión completa cancelación de la palabra clave, de la clave RSA o de la clave criptográfica, que corresponde el estándar de seguridad actual y de los otros parámetros importantes, que se memorizan en el aparato de configuración, mediante el entorno de ejecución seguro.

[0013] Según la invención la autenticación se realiza entre el aparato de configuración y el aparato por configurar preferiblemente mediante la codificación PGP, donde para este fin cada aparato necesita una clave.
La clave correspondiente del aparato de configuración se ha elaborado de tal manera que después de un lapso de tiempo prefijado esta pierde su validez y está memorizada en el aparato de configuración por medio del entorno de ejecución seguro.

[0014] Las clave RSA o la clave criptográdica, que corresponde al estándar de seguridad actual, sirve para hacer posible el acceso al aparato por configurar por medio de un protocolo SSH, particularmente para el caso de que la palabra clave no se pueda introducir o no se pueda comprobar su validez.

[0015] Una vez realizada la autenticación, para la transmisión de una configuración prefijada al aparato por configurar, se transmite preferiblemente al aparato por configurar un archivo ejecutable en una memoria temporal del aparato por configurar, donde la orden para la realización del fichero ejecutable se introduce por medio del aparato de configuración mediante un protocolo de red SSH a través de un puerto de ethernet emulado.

[0016] La clave RSA o la clave criptográfica, que corresponde a los estándares de seguridad actuales, se puede generar durante el procedimiento de configuración por medio del entorno de ejecución seguro del aparato de configuración o mediante una clave memorizada por medio del entorno de ejecución seguro.
Al final del procedimiento de configuración se borran todos los archivos del aparato de configuración, con excepción del archivo que contiene toda la información de configuración, después de que ha sido transmitida al servidor.

[0017] A través de la concepción según la invención se realiza de una manera sencilla una instalación, donde no son conocidos por el usuario la palabra clave y otros parámetros pertinentes a la seguridad.
Además, la contraseña, la clave RSA o la clave criptográfica, que corresponden a los estándares de seguridad actuales y otros parámetros importantes prefijados, están protegidos contra accesos por parte de personas no autorizadas.

[0018] La invención se explica más en detalle a modo de ejemplo a continuación tomando las figuras anexas.
Se muestran:

Figura 1: una representación esquemática de los componentes necesarios para la realización del procedimiento;

Figura 2: un flujograma para la ilustración de los pasos del procedimiento según la invención con ocasión de la conexión entre el aparato por configurar y el aparato de configuración; y

Figura 3: un flujograma para la ilustración de los pasos del procedimiento según la invención con ocasión de la conexión entre el aparato de configuración y un servidor.

[0019] Según la invención y con referencia a la figura 1 para la ejecución del procedimiento se usa un aparato de configuración 1, que se puede conectar al aparato 2 por configurar, que en el ejemplo mostrado se realiza como distribuidor automático, donde la conexión puede ser por cable o inalámbrica, p.ej. a través de WLAN.

[0020] El aparato de configuración 1 presenta una CPU propia, medios de almacenamiento y software y comprende un llamado entorno de ejecución seguro 3.
Además, el aparato de configuración 1 se puede conectar por medio de otro ordenador 4 por medio de una conexión de red segura, que puede ser una conexión VPN a través de internet, a un servidor 5 que comprende un entorno de ejecución seguro para el objetivo de la comunicación de datos.

[0021] Al principio del procedimiento, para la configuración de aparatos electrónicos y especialmente para la configuración de componentes de un sistema de control de acceso para personas o vehículos, como se ilustra en la figura 2, después de la puesta en marcha del aparato de configuración 1, el aparato de configuración 1 se conecta con el aparato 2 por configurar para el objetivo de la comunicación de datos de forma inalámbrica o por cable, donde a continuación se realiza una autenticación recíproca, preferiblemente mediante una codificación PGP y donde una vez efectuada la autenticación mediante el entorno de ejecución seguro 3 del aparato de configuración 1, se transmite una configuración prefijada al aparato 2 por configurar.
La configuración comprende ajustes de red y variables del entorno; a este respecto un usuario puede vigilar el proceso mediante un dispositivo de visualización conectable al aparato de configuración 1 y puede realizar cambios manualmente mediante un dispositivo de entrada conectable al aparato de configuración 1.
A este respecto, se otorga una dirección IP sin tener conocimiento de la dirección MAC del aparato 2 por configurar.

[0022] En una fase que sigue se lee o genera una clave RSA para posibilitar el acceso al aparato por configurar por un protocolo SSH mediante el entorno de ejecución seguro 3 del aparato de configuración 1 y se transmite al aparato por configurar 2 y a continuación se verifica, donde seguidamente se lee o genera una contraseña mediante el entorno de ejecución seguro 3 del aparato de configuración 1, transmitiéndose dicha contraseña mediante una conexión cifrada al aparato por configurar 2 y se comprueba mediante una conexión cifrada y una introducción automática de la contraseña.

[0023] En una fase próxima se crea un archivo que contiene toda la información de configuración, por ejemplo, direcciones IP y MAC para la documentación del procedimiento de configuración y se almacena fuera del entorno de ejecución seguro 3 en el aparato de configuración 1, donde después de crear el archivo se termina la conexión entre el aparato de configuración 1 y el aparato por configurar 2.

[0024] A continuación, y tomando como referencia la figura 3, se crea una conexión para la comunicación de datos entre el aparato de configuración 1 y otro ordenador 4, donde una vez efectuada la autenticación recíproca, se crea una conexión de red segura por medio de otro ordenador 4 a un servidor 5 y donde después de realizar una autenticación recíproca entre el aparato de configuración 1 y el servidor 5, la contraseña, la clave RSA y otros parámetros prefijados se transmiten por medio del entorno de ejecución seguro 3 del aparato de configuración 1 a un entorno de ejecución seguro sobre el servidor 5 mediante la conexión de red segura.

[0025] En una fase que sigue se verifican la integridad de la transmisión de la contraseña, de la clave RSA y de los otros parámetros importantes, donde una vez que ha ocurrido la transmisión completa, estos datos se borran en el aparato de configuración 1. En caso de que la transmisión no haya sido completa, se repite el proceso hasta que la transmisión se ha realizado completamente.

[0026] El método según la invención se realiza de una manera ventajosa para la configuración de componentes de un sistema de control de acceso para personas o vehículos.

REIVINDICACIONES

1. Método para la configuración de aparatos electrónicos y especialmente para la configuración de componentes de un sistema de control de acceso para personas o vehículos, **caracterizado por el hecho de que** se usa un aparato de configuración (1), que se puede conectar al aparato por configurar (2) para el objetivo de la comunicación de datos, que presenta una CPU propia, medios de almacenamiento y software y comprende un entorno de ejecución seguro (3) y mediante otro ordenador (4) se puede conectar mediante una conexión de red segura con un servidor (5) que comprende un entorno de ejecución seguro para el objetivo de la comunicación de datos, donde al principio del método el aparato de configuración (1) se conecta al aparato por configurar (2) para el objetivo de la comunicación de datos y a continuación se realiza una autenticación recíproca, donde una vez realizada la autenticación mediante el entorno de ejecución seguro (3) del aparato de configuración (1), se transmite una configuración prefijada al aparato por configurar (2), que comprende la configuración ajustes de red y variables del entorno, donde a continuación y mediante el entorno de ejecución seguro (3) del aparato de configuración (1) se lee o genera mediante un protocolo SSH una clave RSA o una clave criptográfica, que corresponde el estándar de seguridad actual, para permitir el acceso al aparato por configurar, se transmite al aparato por configurar (2) y a continuación se verifica, donde en una fase que sigue, mediante el entorno de ejecución seguro (3) del aparato de configuración (1) se lee o genera una contraseña, que se transmite mediante una conexión cifrada al aparato por configurar (2) y se comprueba mediante una conexión cifrada y una introducción automática de la contraseña, donde a continuación se crea un archivo que contiene toda la información referente a la configuración y se memoriza fuera del entorno de ejecución seguro (3) en el aparato de configuración (1), donde después de crear el archivo se termina la conexión entre el aparato de configuración (1) y el aparato por configurar (2), donde en una fase que sigue se crea una conexión para la comunicación de datos entre el aparato de configuración (1) y otro ordenador (4), donde una vez realizada la autenticación recíproca, se crea una conexión de red segura a un servidor (5) por medio de otro ordenador (4), y después de realizar una autenticación recíproca entre el aparato de configuración (1) y el servidor (5), la contraseña, la clave RSA o la clave criptográfica, que corresponde a los estándares de seguridad actuales y los otros parámetros prefijados se transmiten mediante el entorno de ejecución seguro (3) del aparato de configuración (1) a un entorno de ejecución seguro sobre el servidor (5) por medio de la conexión de red segura y donde una vez que ha tenido lugar la transmisión completa, estos datos son suprimidos en el aparato de configuración (1).

2. Método según la reivindicación 1, **caracterizado por el hecho de que** para transmitir la configuración prefijada al aparato por configurar (2) se transmite un archivo ejecutable sobre una memoria temporal del aparato por configurar (2), donde la orden para la realización del archivo ejecutable se introduce por medio del aparato de configuración (1) mediante un protocolo de red SSH a través de un puerto de Ethernet emulado.

3. Método según la reivindicación 1 o 2, **caracterizado por el hecho de que** la autenticación se realiza entre el aparato de configuración (1) y el aparato por configurar (2) mediante una codificación PGP, donde la clave correspondiente del aparato de configuración (1) se elabora de tal manera, que después de un periodo de tiempo prefijado pierde su validez.

4. Método según la reivindicación 1 o 2, **caracterizado por el hecho de que** el aparato de configuración (1) se realiza como lápiz USB.

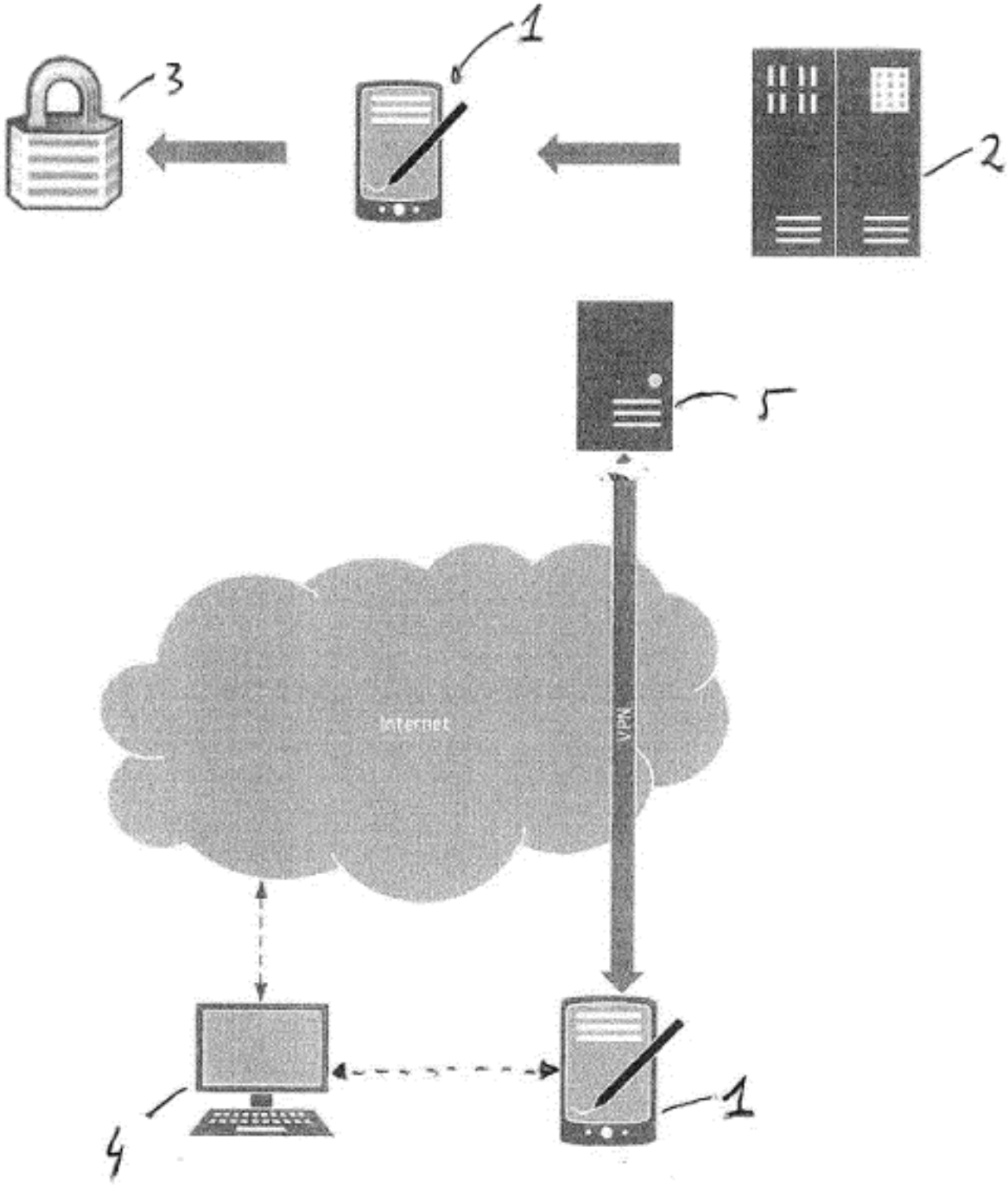

Figura 1

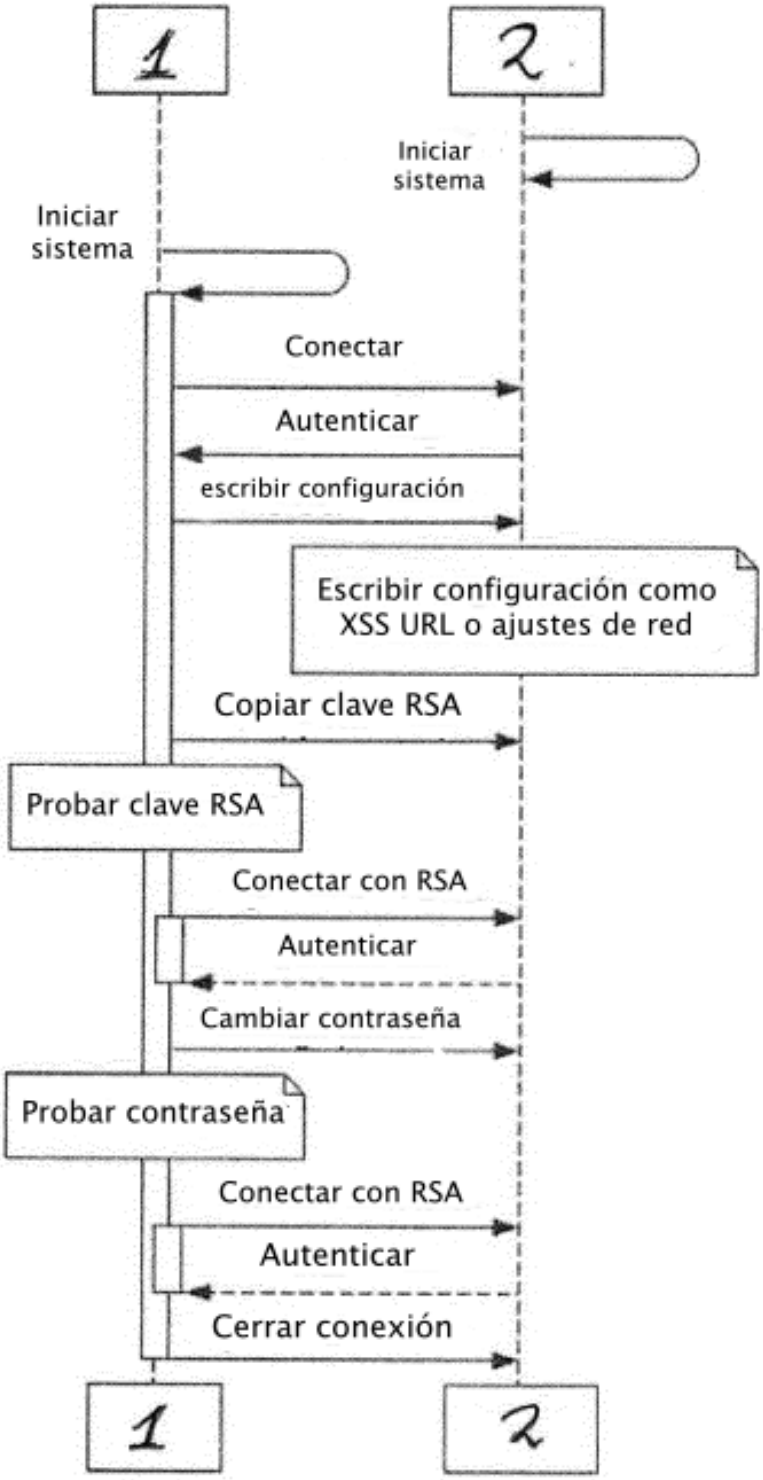
1
2
Iniciar sistema
Iniciar sistema
Conectar
Autenticar
escribir configuración
Escribir configuración como XSS URL o ajustes de red
Copiar clave RSA
Probar clave RSA
Conectar con RSA
Autenticar
Cambiar contraseña
Probar contraseña
Conectar con RSA
Autenticar
Cerrar conexión
1
2

Figura 2

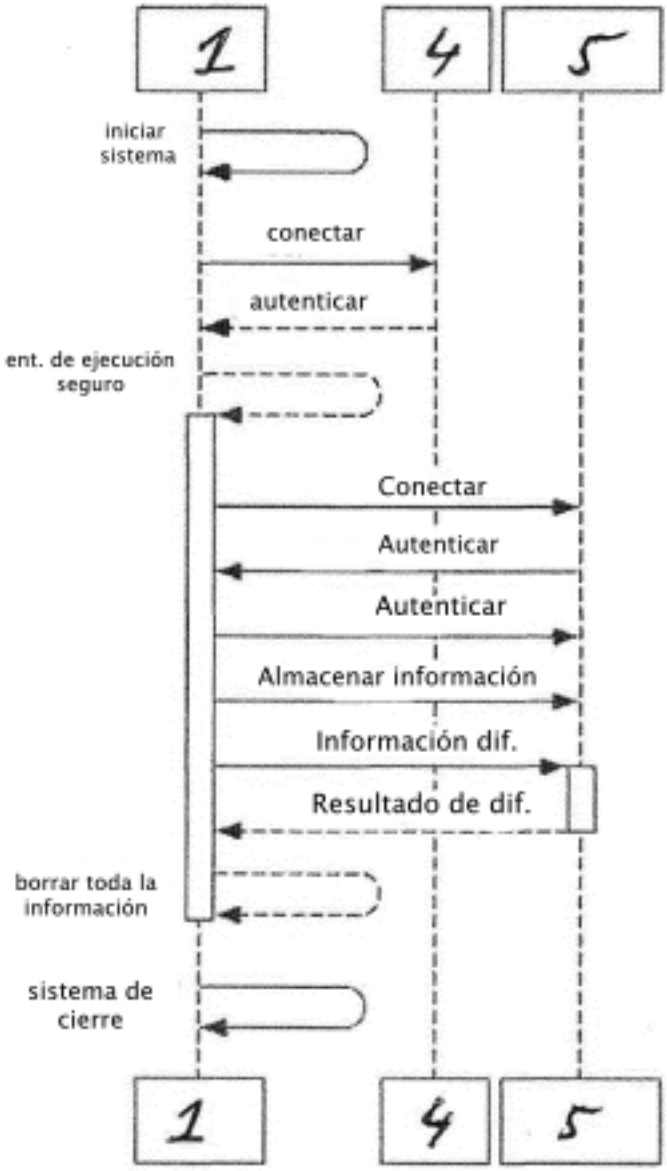
1
4
5
iniciar sistema
conectar
autenticar
ent. de ejecución seguro
Conectar
Autenticar
Autenticar
Almacenar información
Información dif.
Resultado de dif.
borrar toda la información
sistema de cierre
1
4
5

Figura 3