

**MÉTODO PARA OPERAR UN SISTEMA DE CONTROL DE ACCESO QUE
COMPRENDE UN SERVIDOR, AL MENOS UN DISPOSITIVO DE
CONTROL DE ACCESO Y AL MENOS UN DISPOSITIVO DE PUNTO DE
VENTA PARA PERMISOS DE ACCESO PARA EL ÁREA CUBIERTA POR
EL SISTEMA DE CONTROL DE ACCESO**

5

La presente invención se refiere a un método para operar un sistema de control de acceso que comprende un servidor, al menos un dispositivo de control de acceso y al menos un dispositivo de punto de venta para permisos de acceso para el área cubierta por el sistema de control de acceso de acuerdo con el preámbulo de la reivindicación 1.

De la técnica anterior, se conocen sistemas de control de acceso que tienen un servidor y al menos un dispositivo de control de acceso que se conecta al servidor para el propósito de comunicación de datos. Para la venta de los permisos de acceso para el área cubierta por el sistema de control de acceso, se proporcionan puntos de venta, en los que cuando se compra un permiso de acceso, el permiso de acceso se codifica en un medio de cliente por medio de un dispositivo de punto de venta conectado al servidor para el propósito de comunicación de datos usando un dispositivo de cifrado, por medio de una norma de RFID, preferentemente la norma ISO 15693. En este caso, el permiso de acceso se genera y cifra en el servidor.

De acuerdo con la técnica anterior los algoritmos para la generación y cifrado de privilegios de acceso se almacenan en el servidor y no se distribuyen al dispositivo de punto de venta conectado al servidor para el propósito de comunicación. Los permisos de acceso se generan y cifran en el servidor y se codifican en el medio de cliente a través del dispositivo de punto de venta conectado al servidor para el propósito de comunicación de datos, en la que después de la codificación de la información de permisos de acceso relativa a la validez de los respectivos permisos de acceso se transmite desde el servidor al dispositivo de control de accesos.

Desventajosamente, en el evento de un fallo de red, es decir en un modo fuera de línea del dispositivo de punto de venta, no pueden venderse permisos de acceso, ya que de acuerdo con la técnica estos no pueden generarse y cifrarse por los puestos de venta.

El objeto de la presente invención es especificar un método para operar un sistema de control de acceso que comprende un servidor, al menos un dispositivo de control de acceso y al menos un dispositivo de punto de venta para permisos de acceso para el área cubierta por el sistema de control de acceso, mediante cuya ejecución para el caso cuando un dispositivo de punto de venta de un sistema de control de acceso está en un modo fuera de línea, se mantiene la operación del sistema de control de acceso y, en particular, la venta de permisos de acceso.

Este objeto se consigue mediante las características de la Reivindicación de Patente. Una extensión ventajosa es la materia objeto de la reivindicación dependiente.

En consecuencia, se propone un método para operar un sistema de control de acceso que comprende un servidor, al menos un dispositivo de control de acceso y al menos un dispositivo de punto de venta para permisos de acceso para el área cubierta por el sistema de control de acceso, en cuyo contexto el algoritmo para generar y cifrar los permisos de acceso se instala en el al menos un dispositivo de punto de venta, en el que el algoritmo puede ejecutarse de forma local únicamente, es decir en el al menos un dispositivo de punto de venta, si se desbloquea usando una clave.

De acuerdo con la invención, cuando se enciende o conecta un dispositivo de punto de venta, la clave para desbloquear el algoritmo para generar y cifrar permisos de acceso, que se instala en el dispositivo de punto de venta, se transfiere desde el servidor al dispositivo de punto de venta, en el que, en el caso de en línea, es decir cuando el dispositivo de punto de venta se conecta al servidor, el dispositivo de punto de venta solicita un permiso de acceso desde el servidor, que se genera y cifra en el servidor y se transmite desde el servidor al dispositivo de punto de venta, en el que el permiso de acceso se codifica en un medio de cliente usando un dispositivo codificador del dispositivo de punto de venta. Posteriormente, la información relativa a la validez del permiso de acceso codificado se transmite desde el servidor al, al menos un dispositivo de control de acceso, en el que para el propósito de control de acceso el permiso de acceso se lee por el respectivo dispositivo de control de acceso y la validez del permiso de acceso se verifica sobre la base de la información transmitida desde el servidor.

En el caso fuera de línea, es decir cuando un dispositivo de punto de

venta no está conectado al servidor, el algoritmo instalado en el dispositivo de punto de venta se ejecuta usando la clave para desbloquear el algoritmo instalado en el dispositivo de punto de venta, en el que por medio del algoritmo instalado en el dispositivo de punto de venta se genera, cifra y etiqueta un permiso de acceso como un permiso de acceso generado fuera de línea, en el que este permiso de acceso se codifica a continuación en un medio de cliente usando el dispositivo de cifrado del dispositivo de punto de venta.

Si se realiza un control de acceso mientras el dispositivo de punto de venta no está conectado al servidor, el permiso de acceso generado fuera de línea se lee por un dispositivo de control de acceso, en el que sobre la base del etiquetado como un permiso de acceso generado fuera de línea se reconoce como tal, en el que la validez del permiso de acceso se verifica sobre la base de los datos cifrados por el dispositivo de punto de venta.

Si el dispositivo de punto de venta está posteriormente en un modo en línea, que corresponde al estado de operación normal, la información relativa a los permisos de acceso generados por el dispositivo de punto de venta en el modo fuera de línea se transmite desde el dispositivo de punto de venta al servidor, que a su vez transmite la información relativa a la validez de los permisos de acceso al, al menos un dispositivo de control de acceso.

Si después de que el dispositivo de punto de venta ha cambiado al modo en línea se produce un proceso de control de acceso con un permiso de acceso generado por el dispositivo de punto de venta en el modo fuera de línea, el permiso de acceso generado fuera de línea se lee del medio de cliente por el dispositivo de control de acceso, en el que se codifica un permiso de acceso en el medio de cliente basándose en la información transmitida por el servidor y la validez del permiso de acceso se verifica a continuación.

Como parte de una extensión de la invención, se prevé que si se realiza un control de acceso mientras el dispositivo de punto de venta no está conectado al servidor, una validez limitada en el tiempo, al saber la información que el permiso de acceso vuelve inválida después de un tiempo especificado, se codifica en el medio de cliente mediante el dispositivo de control de acceso, en el que la validez limitada en el tiempo se elimina si se produce una operación de control de acceso después de que el dispositivo

de punto de venta ha cambiado al modo en línea.

A continuación, se describe una realización de la invención en mayor detalle sobre la base de la figura adjunta, que muestra un diagrama de secuencia para ilustrar las características del método de acuerdo con la invención.

De acuerdo con la invención el algoritmo para generar y cifrar los permisos de acceso se instala en el al menos un dispositivo de punto de venta del sistema de control de acceso, en el que el algoritmo instalado en el al menos un dispositivo de punto de venta puede ejecutarse únicamente si se desbloquea usando una clave. Haciendo referencia a la figura adjunta, cuando se enciende o conecta un dispositivo de punto de venta 1, la clave para desbloquear el algoritmo instalado en el dispositivo de punto de venta 1 para generar y cifrar permisos de acceso se transmite desde el servidor 3 al dispositivo de punto de venta 1 (etapa 1).

Si el dispositivo de punto de venta 1 está en el modo en línea, el dispositivo de punto de venta 1 solicita del servidor 3 un permiso de acceso, que se genera y cifra en el servidor 3 y se transmite desde el servidor 3 al dispositivo de punto de venta (etapa 2), en el que el permiso de acceso se codifica a continuación en un medio de cliente (etapa 3) usando un dispositivo de cifrado 2 del dispositivo de punto de venta 1.

Posteriormente, la información relativa a la validez del permiso de acceso codificado se transmite desde el servidor 3 al al menos un dispositivo de control de acceso 4 del sistema de control de acceso (etapa 4), en el que para el propósito de control de acceso el permiso de acceso se lee por el respectivo dispositivo de control de acceso (etapa 5) y la validez del permiso de acceso se verifica sobre la base de la información transmitida por el servidor 3.

Cuando un dispositivo de punto de venta está en un modo fuera de línea, el algoritmo instalado en el dispositivo de punto de venta 1 se ejecuta usando la clave para desbloquear el algoritmo instalado en el dispositivo de punto de venta 1, en el que por medio del algoritmo instalado en el dispositivo de punto de venta 1 se genera, cifra y etiqueta un permiso de acceso como un permiso de acceso generado fuera de línea (etapa 7), en el que este permiso de acceso se codifica a continuación en un medio de cliente por el dispositivo de cifrado del dispositivo de punto de venta (etapa

8).

En el evento de un control de acceso mientras el dispositivo de punto de venta 1 no está conectado al servidor 3, el permiso de acceso generado fuera de línea se lee (etapa 9) por un dispositivo de control de acceso, en el que sobre la base del etiquetado como un permiso de acceso generado fuera de línea se reconoce como tal, cuya validez se verifica (etapa 10) sobre la base de los datos cifrados por el dispositivo de cifrado 2 del dispositivo de punto de venta 1 y una limitación de validez limitada en el tiempo, al saber la información que el permiso de acceso vuelve inválida después de un tiempo especificado, se codifica en el medio de cliente (etapa 11).

Si el dispositivo de punto de venta 1 cambia a continuación al modo en línea, la información relativa a los permisos de acceso generados por el dispositivo de punto de venta 1 en el modo fuera de línea se transmite desde el dispositivo de punto de venta 1 al servidor 3 (etapa 12), donde el servidor 3 transmite la información acerca de la validez de los permisos de acceso al al menos un dispositivo de control de acceso 4 del sistema de control de acceso (etapa 13).

En el evento de un control de acceso posterior con un permiso de acceso generado por el dispositivo de punto de venta 1 en el modo fuera de línea, es decir sin una conexión al servidor 3, el permiso de acceso generado fuera de línea se lee por un dispositivo de control de acceso (etapa 14), en el que si se codificó una validez limitada en el tiempo en el medio de cliente, que significa que el medio de cliente se verificó por un dispositivo de control de acceso 4 durante el modo fuera de línea del dispositivo de punto de venta 1, la validez limitada en el tiempo se elimina y se codifica un permiso de acceso en el medio de cliente basándose en la información transmitida desde el servidor 3 (etapa 15), en el que la validez del permiso de acceso se comprueba a continuación.

Si el medio de cliente no se verificó durante el modo fuera de línea del dispositivo de punto de venta 1, es decir si no se codifica ninguna validez limitada en el tiempo en el medio de cliente, se codifica un permiso de acceso en el medio de cliente (etapa 16) basándose en la información transmitida desde el servidor relativa a la validez del permiso de acceso, en el que la validez del permiso de acceso se comprueba a continuación.