(19) OFICINA ESPAÑOLA DE PATENTES Y MARCAS

ESPAÑA

(11) Número de publicación: **2 398 894**

(51) Int. CI.:

H04L 29/06 (2006.01)
G06F 21/00 (2006.01)

(12) TRADUCCIÓN DE PATENTE EUROPEA T3

(96) Fecha de presentación y número de la solicitud europea: **22.06.2010 E 10166767 (3)**

(97) Fecha y número de publicación de la concesión europea: **31.10.2012 EP 2299644**

(54) Título: **Procesamiento de datos con autenticación a posteriori**

(30) Prioridad:

29.06.2009 FR 0954433

(45) Fecha de publicación y mención en BOPI de la traducción de la patente:
22.03.2013

(73) Titular/es:

FRANCE TÉLÉCOM (100.0%)
78 rue Olivier de Serres
75015 Paris , FR

(72) Inventor/es:

GIORDANI, MICHEL;
RIGOLLE, YOANN y
GARNIER DE FALLETANS, GUILLAUME

(74) Agente/Representante:

LINAGE GONZÁLEZ, Rafael

DESCRIPCIÓN

Procesamiento de datos con autenticación a posteriori

La invención se refiere al ámbito del procesamiento de datos informáticos y, más concretamente, a un procedimiento de datos y un dispositivo asociado.

El procesamiento de datos informáticos sensibles plantea distintos problemas. En particular, en el ámbito médico, en Francia, la legislación impone una fuerte securización de los datos informáticos médicos y recomienda para ello que los profesionales de la salud utilicen una tarjeta con microprocesador como medio de autenticación fuerte para acceder a dichos datos médicos.

La autenticación de la entidad que requiere un acceso a datos informáticos es en efecto un medio privilegiado para garantizar la securización de los datos informáticos sensibles. La autenticación simple (típicamente con identificador y simple contraseña) se emplea de forma corriente pero no ofrece un nivel de seguridad suficiente para asegurar la protección de los datos informáticos sensibles. Su principal debilidad reside en la facilidad con la que la identidad de la entidad puede usurparse mediante, por ejemplo, técnicas de ataque basadas en la ingeniería social que permiten encontrar la contraseña definida por el usuario.

Por lo tanto, es necesario utilizar una autenticación fuerte para una protección eficaz de datos informáticos sensibles. El uso de la tarjeta con microprocesador, asociada a un segundo dato de autenticación del tipo código PIN, es una solución de autenticación fuerte que permite, por ejemplo, obtener un nivel de seguridad suficiente para controlar el acceso a datos informáticos sensibles.

Ahora bien, dicha autenticación fuerte impone distintas limitaciones al usuario: debe llevar con él su medio de autenticación (tarjeta), disponer de un lector adecuado para este medio de autenticación, así como un terminal compatible con el método de autenticación requerido para acceder al servicio. Por ello, no es sistemáticamente posible para dicho usuario autenticarse de manera adecuada en un servidor que controla el acceso a datos, especialmente cuando dicho usuario realiza una actividad ambulante y se desplaza con frecuencia sin poder llevar con él todo el material necesario.

Por lo tanto, los inventores han comprobado la necesidad de disponer de una técnica de securización del acceso a datos informáticos sensibles que presente un nivel de seguridad equivalente al proporcionado por una autenticación fuerte, sin por ello ser tan limitativo como una autenticación fuerte.

El documento US 2008/086767 describe un método de procesamiento de datos en el que un primer usuario autenticado puede solicitar efectuar un cambio en unos datos personales. Sin embargo, para ello, es necesaria la autorización de un segundo usuario autenticado.

Uno de los objetivos de la invención es remediar problemas, inconvenientes o insuficiencias del estado de la técnica y/o aportarle mejoras.

La invención se refiere, según un primer modo de realización, a un primer procedimiento de procesamiento de datos aplicado por un servidor, según la reivindicación 1.

Este primer modo de realización corresponde a un método de autenticación fuerte a posteriori.

Según este primer modo de realización de la invención, un primer usuario puede beneficiarse de un primer acceso a un servicio de procesamiento de datos sensibles. Las operaciones solicitadas al acceder sin autenticación fuerte y, por lo tanto, los datos resultantes de estas operaciones solo se validan, es decir se ejecutan efectivamente, en un segundo momento a petición de un segundo usuario (en general, el mismo primer usuario o su delegado), en un acceso posterior con autenticación fuerte.

La invención consigue este resultado mediante separación entre una primera fase, en la que se definen, incluso se simulan, las operaciones a ejecutar, y una segunda fase en la que se validan dichas operaciones, es decir se ejecutan efectivamente.

Por motivos de seguridad, se comprueba además la relación entre el primer usuario conectado en el primer acceso y el segundo usuario conectado en el segundo acceso, antes de validar las operaciones solicitadas por el primer usuario, con objeto de garantizar que solo un segundo usuario autorizado (en general el mismo primer usuario o su delegado) pueda validar dichas operaciones.

Se garantiza la seguridad por el hecho de que se otorga la confianza en las operaciones de procesamiento definidas a posteriori, durante la validación de dichas operaciones tras una autenticación fuerte.

Un segundo modo de realización corresponde a un segundo procedimiento de procesamiento de datos aplicado por

un servidor, que incluye

- una etapa de recepción, en una primera sesión de comunicación establecida con dicho servidor, de una solicitud formulada por un primer usuario para autorizar por lo menos una operación de procesamiento a ejecutar con unos primeros datos;

- una etapa de ejecución de una operación de procesamiento con dichos primeros datos, en una segunda sesión de comunicación establecida con dicho servidor posteriormente a dicha primera sesión por un segundo usuario,

estando destinada dicha etapa de ejecución a iniciarse con la condición, por una parte, de que el primer usuario haya sido autenticado mediante un método de autenticación fuerte en la primera sesión y, por otra, que se haya comprobado por lo menos una relación entre el primero y el segundo usuario.

Este segundo modo de realización corresponde a un método de autenticación fuerte a priori.

En este segundo modo de realización, un primer usuario puede beneficiarse de un acceso a un servicio de procesamiento de datos sensibles con autenticación fuerte durante la cual este primer usuario requiere una autorización para ejecutar operaciones, en un acceso posterior sin autenticación fuerte.

En este caso, se confía a priori para acciones a definir y validar en una sesión posterior establecida con un nivel de confianza más bajo.

También en este caso, por motivos de seguridad, se comprueba además una relación entre el primer usuario conectado en el primer acceso y el segundo usuario conectado en el segundo acceso, antes de validar las operaciones solicitadas por el segundo usuario, con el fin de garantizar que solo puedan validarse las operaciones solicitadas por un segundo usuario autorizado.

Según un modo de realización del segundo procedimiento, la etapa de ejecución está destinada a aplicarse si se comprueba, en el momento de dicha ejecución, una condición formulada por el primer usuario en la primera sesión.

Esta condición pretende limitar los riesgos de violación de los datos mediante esta condición impuesta por este primer usuario: por ejemplo, mediante limitación de la naturaleza de las operaciones solicitadas o limitación a un período de tiempo predefinido.

El primero y el segundo procedimiento se prestan a distintos modos de realización.

Según un primer modo de realización del primero o segundo procedimiento, dicha relación se comprueba si se verifica una relación entre una primera información propia del primer usuario y una segunda información propia del segundo usuario. Se comprueba así que ambos usuarios están relacionados entre ellos mediante informaciones que cada uno posee.

Según otro modo más de realización del primero o segundo procedimiento, dicha primera, respectivamente segunda, información se proporciona a dicho servidor por parte del primero, respectivamente segundo, usuario durante dicha primera, respectivamente segunda, sesión. Esto permite reforzar la seguridad y los riesgos de intervención de un usuario pirata: la primera información es por ejemplo un secreto que posee el primer usuario, compartida con el segundo usuario, y que debe proporcionar el segundo usuario.

Según otro modo de realización del primero o segundo procedimiento, dicha relación se verifica si el segundo usuario ha delegado derechos al primer usuario. Esto permite a varios usuarios cooperar para la realización de operaciones con datos.

Según otro modo más de realización del primero o del segundo procedimiento, dicha relación se verifica si un identificador del primer usuario es idéntico a un identificador del segundo usuario. En algunos casos, se impone una identidad estricta entre ambos usuarios.

Los distintos modos de realización mencionados anteriormente pueden combinarse entre ellos para la aplicación de la invención; especialmente, es posible prever que deben verificarse varias relaciones entre ambos usuarios: igualdad entre identificadores o delegación de derechos, con o sin relación entre dos informaciones propias, u otra condición adicional.

Según una implementación preferida, las distintas etapas del procedimiento según la invención se aplican por medio de un software o programa de ordenador, incluyendo dicho software instrucciones destinadas a ser ejecutadas por un microprocesador de datos de un dispositivo de procesamiento de datos y habiéndose diseñado para comandar la ejecución de las distintas etapas de este procedimiento.

En consecuencia, la invención afecta asimismo a un programa, susceptible de ser ejecutado por un ordenador o por

un procesador de datos, incluyendo este programa instrucciones para comandar la ejecución de las etapas de un procedimiento como el mencionado anteriormente.

Este programa puede utilizar cualquier lenguaje de programación, y ser en forma de código fuente, código objeto, o código intermedio entre código fuente y código objeto, como en una forma en parte compilada, o en cualquier otra forma deseable.

La invención afecta asimismo a un soporte de información legible por un ordenador o un procesador de datos, que incluye instrucciones de un programa como se ha mencionado anteriormente.

El soporte de información puede ser cualquier entidad o dispositivo capaz de almacenar el programa. Por ejemplo, el soporte puede incluir un medio de almacenamiento, como una ROM, por ejemplo un CD ROM o una ROM de circuito microelectrónico, o un medio de grabación magnético, por ejemplo un disquete (floppy disc) o un disco duro.

Por otra parte, el soporte de información puede ser un soporte transmisible, como una señal eléctrica u óptica, que puede trasladarse por medio de un cable eléctrico u óptico, por radio o por otros medios. El programa según la invención puede especialmente cargarse en una red del tipo Internet.

Alternativamente, el soporte de información puede ser un circuito integrado en el que se incorpora el programa, habiéndose adaptado el circuito para ejecutar o para ser utilizado en la ejecución del procedimiento en cuestión.

Según otra implementación, la invención se aplica por medio de componentes de software y/o materiales. Con esta óptica, el término módulo puede corresponder en este documento tanto a un componente software como a un componente material o a un componente material programable, con o sin procesador integrado.

Un componente software corresponde a uno o varios programas de ordenador, uno o varios subprogramas de un programa o, de manera más general, a cualquier elemento de un programa o un software capaz de aplicar una función o conjunto de funciones, según lo que se describe a continuación para el módulo afectado. Del mismo modo, un componente material corresponde a cualquier elemento de un conjunto material (o hardware) capaz de aplicar una función o un conjunto de funciones, según lo que se describe a continuación para el módulo afectado.

La invención se refiere, según un segundo aspecto, a un primer dispositivo de procesamiento de datos, que incluye

- medios para recibir, en una primera sesión de comunicación establecida, una solicitud formulada por un primer usuario que define por lo menos una operación de procesamiento a ejecutar con unos primeros datos;

- medios de ejecución de una operación de procesamiento con dichos primeros datos, durante una segunda sesión de comunicación establecida con dicho servidor posteriormente a dicha primera sesión para un segundo usuario;

estando destinados dichos medios de ejecución a ser activados con la condición, por una parte, de que el segundo usuario haya sido autenticado mediante un método de autenticación fuerte en la segunda sesión y, por otra, que se haya verificado una relación entre el primero y el segundo usuario.

Este primer dispositivo emplea una autenticación fuerte a posteriori.

Un segundo dispositivo de procesamiento de datos incluye

- medios para recibir, en una primera sesión de comunicación establecida con dicho servidor, una solicitud formulada por un primer usuario para autorizar por lo menos una operación de procesamiento a ejecutar con unos primeros datos;

- medios de ejecución de una operación de procesamiento con dichos primeros datos, en una segunda sesión de comunicación establecida con dicho servidor posteriormente a dicha primera sesión para un segundo usuario,

estando destinados dichos medios de ejecución a ser activados con la condición, por una parte, de que el primer usuario haya sido autenticado mediante un método de autenticación fuerte en la primera sesión y, por otra, de que se haya verificado por lo menos una relación entre el primero y el segundo usuario.

Este segundo dispositivo emplea una autenticación fuerte a priori.

Las ventajas mencionadas para el primero y el segundo procedimiento pueden transponerse respectivamente al primero y al segundo dispositivo.

Otros objetivos, características y ventajas de la invención aparecerán mediante la siguiente descripción, proporcionada únicamente a título de ejemplo no limitativo y realizada con referencia a los dibujos adjuntos, en los cuales:

- la figura 1 representa de forma esquemática un sistema de comunicación que incorpora un dispositivo según la invención;

- la figura 2 representa un organigrama de un primer modo de realización del procedimiento según la invención;

- las figuras 3a y 3b representan el contenido y la disposición de espacios de memoria utilizada para la aplicación del procedimiento según la invención.

La invención se describe más en detalle con referencia a la figura 1 en el contexto de su aplicación a un servicio de procesamiento de datos médicos para profesionales de la salud. Este servicio se pone en práctica por medio de un servidor AS, con forma típicamente de servidor Web, accesible mediante una red de telecomunicación RS. Dicho servidor es accesible desde un terminal T conectado a la red RS, terminal a partir del cual un usuario puede enviar sus solicitudes para pedir la ejecución de una operación de procesamiento de datos, enviar y/o recibir datos.

Por medio de este servidor, y a petición de un usuario, se pueden llevar a cabo distintas operaciones de procesamiento de datos:

- recepción y/o almacenamiento de datos proporcionados por el usuario;

- edición y/o modificación de datos almacenados;

- transmisión de datos a un usuario o una entidad;

- eliminación de datos almacenados;

- etc.

Los datos se almacenan en una base de datos DB, asociada al servidor aplicativo AS. Los datos almacenados son, por ejemplo:

- datos médicos sobre el estado de salud de un paciente;

- formularios de atención sanitaria a transmitir a la seguridad social;

- recetas médicas establecidas para un paciente;

- etc.

El servidor AS gestiona derechos de acceso por usuario para los datos almacenados en la base de datos: cada usuario tiene asociado un conjunto de datos para los que dispone de una autorización de acceso, siendo estos datos almacenados, por ejemplo, en un espacio de almacenamiento de datos que le es propio. Por ejemplo, como se muestra en la figura 3a o 3b, un usuario U1 tiene asignado un espacio de almacenamiento ES1 y un usuario U2 tiene asignado un espacio de almacenamiento ES2, teniendo ambos espacios una parte común ES12 para los datos de acceso compartido entre los usuarios U1 y U2.

Se utiliza un método de autenticación para autenticar a cada usuario que solicita efectuar una operación con dichos datos.

Según el método de autenticación elegido para autenticar a un usuario, el nivel de seguridad será más o menos elevado. Un método de autenticación débil se basa en un único factor (por ejemplo, el usuario proporciona una contraseña). Un método de autenticación fuerte se basa en dos factores o más, eligiéndose por ejemplo estos factores en la siguiente relación:

- lo que el usuario conoce (por ejemplo, una contraseña, un código PIN, una frase secreta, etc.);

- lo que el usuario posee (por ejemplo, una tarjeta magnética, una tarjeta RFID, una llave USB, una PDA, una tarjeta con microprocesador, etc.);

- lo que el usuario es (para una persona física, cualquier huella biométrica característica del usuario, huella dactilar, huella retiniana, estructura de la mano, estructura ósea del rostro, etc.);

- lo que el usuario sabe hacer (para una persona física, firma manuscrita, reconocimiento de la voz, un tipo de cálculo conocido solo por el usuario, etc.).

En el ejemplo de aplicación de la invención descrito aquí, se supone que el nivel de confidencialidad de los datos

procesados por el servidor es tal que se requiere una autenticación fuerte como condición previa a la ejecución de una operación con datos que impliquen una escritura (creación, modificación y eliminación) de datos en la base de datos DB. Por el contrario, para una consulta de datos o una operación que implique solo una lectura de datos de la base de datos DB, se supone que una autenticación simple es suficiente para autorizar este tipo de consulta u operación. Así es como se garantiza en todo momento la confianza en los datos sensibles.

El servidor AS ofrece dos modos de acceso a los datos gestionados por dicho servidor:

- un primer modo de acceso, denominado modo altamente securizado, que supone que el usuario conectado sea previamente autenticado mediante un método de autenticación fuerte, denominándose la sesión en este caso sesión altamente securizada;

- un segundo modo de acceso, denominado modo escasamente securizado, que supone que el usuario conectado sea previamente autenticado mediante un método de autenticación débil, sin que se requiera una autenticación fuerte, denominándose la sesión en este caso sesión escasamente securizada.

Durante un acceso en modo altamente securizado, un usuario Ui (U1 respectivamente U2) se beneficia de la totalidad de los derechos de acceso: al mismo tiempo de lectura y escritura sobre los datos del espacio de almacenamiento ESi (ES1 respectivamente ES2) que tiene asociado. Durante dicho acceso, el servidor autoriza y ejecuta todas las operaciones solicitadas por este usuario a petición del usuario.

Durante un acceso en modo escasamente securizado, un usuario Ui se beneficia de derechos de acceso restringidos: únicamente de lectura sobre los datos del espacio de almacenamiento ESi que tiene asociado, pero no de escritura. Durante dicho acceso, solo se autorizan y ejecutan las operaciones que no requieran una escritura de datos de este espacio de almacenamiento ESi. Para las demás operaciones, el usuario puede requerir la ejecución, incluso visualizar su resultado, es decir visualizar los datos resultantes de la operación, pero no validar las operaciones.

En efecto, las operaciones solicitadas por un primer usuario U1 durante un acceso en modo escasamente securizado no se validan inmediatamente. Solo pueden validarse durante una segunda sesión de comunicación, establecida posteriormente a la primera sesión de comunicación por un segundo usuario U1bis, con la condición:

- por una parte, de que esta segunda sesión se establezca en modo altamente securizado, es decir que el segundo usuario U1bis sea autenticado mediante un método de autenticación fuerte;

- por otra parte, de que se verifique una relación predeterminada entre el primero y el segundo usuario U1 y U1bis.

Este mecanismo con dos modos de acceso distintos permite validar a posteriori, durante una sesión altamente securizada, las operaciones solicitadas por un primer usuario U1 durante una sesión anterior escasamente securizada. Este resultado se obtiene desacoplando la fase de definición de las operaciones a ejecutar y la fase de validación de dichas operaciones, requiriéndose la autenticación fuerte únicamente para la fase final, es decir la fase de validación.

El nivel de seguridad del sistema se aproxima al de un sistema que ofreciera únicamente el modo de acceso altamente securizado, dado que solo se validan las operaciones, es decir que se hacen efectivas, con la condición de autenticación fuerte del segundo usuario. Se garantiza de esta manera que solo un usuario debidamente autorizado pueda validar operaciones de procesamiento y modificar los datos almacenados en el servidor. La seguridad se garantiza porque la confianza en las operaciones de procesamiento definidas se otorga a posteriori, durante la validación de dichas operaciones.

Con objeto de realizar una validación a posteriori, el servidor está diseñado para memorizar datos, denominados datos intermedios DINT1, a partir de los cuales una operación solicitada por un primer usuario U1 durante la primera sesión puede validarse, es decir ejecutarse efectivamente, durante la segunda sesión. Estos datos intermedios DINT1 incluyen por ejemplo:

- cuando la operación solicitada es un almacenamiento de datos DATA1 proporcionados por el usuario: los propios datos DATA1 y, opcionalmente, un código que identifique la operación solicitada;

- cuando la operación solicitada es una transmisión a un tercer usuario de datos DATA1 proporcionados por el usuario: los propios datos DATA1 proporcionados y, opcionalmente, un código que identifique la operación solicitada;

- cuando la operación solicitada modifica datos DATA1 (operación de edición, modificación, transformación de datos, etc.): bien los datos DATA1bis resultantes de esta operación, bien los datos DATA1 a modificar en asociación con un código que identifique la operación solicitada;

- cuando la operación solicitada elimina datos DATA1 (operación de eliminación): los datos DATA1 a eliminar en asociación con un código que identifique la operación solicitada.

Los datos intermedios DINT1 definidos de esta forma se almacenan temporalmente en un espacio de memoria propio del usuario U1 que ha formulado la solicitud de ejecución de una operación, y son accesibles únicamente por dicho usuario U1. Este espacio de memoria se denomina aquí espacio de memoria intermedia del usuario U1 y lleva la referencia EIT1 en la figura 3a o 3b. El servidor AS utiliza este espacio de memoria intermedia EIT1 para el almacenamiento de datos intermedios DINT1 relativos a operaciones solicitadas por el usuario U1. El servidor AS proporciona al usuario U1 asociado a este espacio de memoria intermedia una visión del contenido de dicho espacio.

Hasta que una operación con datos DATA1 contenidos en el espacio de almacenamiento ES1 realizada por el usuario U1 no ha sido validada durante una sesión altamente securizada por un usuario U1bis, los demás usuarios solo podrán consultar – suponiendo que tengan acceso a los datos DATA1 – dichos datos DATA1 en el estado en el que se encontraban antes de la ejecución de la operación solicitada por dicho usuario U1. Especialmente, no tendrán acceso al contenido del espacio de memoria intermedia EIT1 del usuario U1.

Durante una sesión en modo de acceso escasamente securizado, un usuario U1 puede solicitar o definir cualquier número de operaciones de procesamiento de datos destinados a ser ejecutados por el servidor AS. Los datos intermedios DINT1 relativos a todas las operaciones definidas por un usuario U1 se almacenan en el espacio de memoria intermedia EIT1 del usuario U1. El servidor AS está diseñado para proporcionar al usuario U1, a partir de estos datos intermedios DINT1, una visión del contenido de dicho espacio de memoria intermedia EIT1: esta visión incluye por ejemplo una relación de las operaciones solicitadas por el usuario U1 y/o los datos resultantes de dichas operaciones y/o los datos a procesar mediante dichas operaciones.

Durante una sesión con modo de acceso altamente securizado, un usuario U1bis, con reserva de que presente una relación predefinida con un usuario U1, puede validar una o varias de las operaciones entre la lista de operaciones solicitadas por dicho usuario U1.

Con este objetivo, si se verifica dicha relación, se muestra a un usuario U1bis dicha lista de operaciones y/o una visión de los datos resultantes de dichas operaciones, con objeto de que pueda seleccionar la o las operaciones que desea validar. Como alternativa, se validan automáticamente todas las operaciones solicitadas por el usuario U1, siempre que el usuario U1bis muestre una relación predefinida con el usuario U1.

Cuando el servidor AS valida operaciones solicitadas por el usuario U1, extrae los datos intermedios DINT1 almacenados en el espacio de memoria intermedia EIT1 del usuario U1 para estas operaciones, y:

- cuando dichos datos intermedios DINT1 contienen datos DATA1bis resultantes de operaciones a validar, el servidor AS copia simplemente dichos datos DATA1bis del espacio de memoria intermedia EIT1 propio del usuario U1 al espacio ES1 de almacenamiento de datos asociado al usuario U1;

- cuando dichos datos intermedios DINT1 contienen una lista de operaciones con códigos que identifican dichas operaciones y los datos DATA1 a los que se aplican estas operaciones, el servidor AS ejecuta las operaciones solicitadas en el orden en el que se han solicitado a partir de dichos datos DATA1 y códigos, y graba los datos DATA1bis resultantes en el espacio ES11 de almacenamiento de datos del usuario U1.

En ambos casos, los datos DATA1bis resultantes de la validación son accesibles, para lectura y escritura, para el usuario U1bis actualmente conectado, así como para cualquier otro usuario autorizado a acceder a dichos datos o al espacio de almacenamiento en el que están almacenados.

Cuando se han modificado los datos iniciales DATA1, dichos datos DATA1 son sustituidos por los datos DATA1bis resultantes.

La invención permite una validación a posteriori de operaciones sensibles y presenta una mayor seguridad que un procedimiento basado únicamente en autenticación simple.

Con objeto de garantizar la seguridad del sistema, se verifica previamente a la validación de las operaciones solicitadas por el usuario U1 una relación predeterminada entre el primero y el segundo usuario U1 y U1bis: de esta manera, solo un segundo usuario U1bis que presente una relación con un primer usuario U1 puede validar operaciones solicitadas por dicho primer usuario, lo que permite garantizar que un usuario dado no pueda validar cualquier operación y mantiene así un control sobre los datos puestos a disposición vía dicho servidor.

Dicha relación se verifica por ejemplo si el primer usuario U1 y el segundo usuario U1bis están identificados mediante un mismo identificador ID1 para el servidor AS: en este caso, los dos usuarios U1 y U1bis son vistos por el servidor AS como un único y mismo usuario. El identificador de un usuario es determinado por el servidor AS sobre la base de los datos de identificación y autenticación proporcionados por dicho usuario en el momento de su

conexión. Dicho identificador es en general distinto del código de identificación (por ejemplo el "login") utilizado como dato de identificación durante la conexión. Poco importa aquí que los usuarios U1 y U1bis sean o no una única y misma persona física: solo importa que estos dos usuarios sean conocidos del servidor AS como un único y mismo usuario "lógico", es decir que sean conocidos con un mismo identificador ID1. En esta óptica, la invención es aplicable al caso en que los datos de identificación y autenticación débil del usuario U1bis (login y contraseña) se transmiten a un usuario U1 que los utiliza para conectarse en modo de acceso no securizado.

Sin embargo, con el fin de preservar el sistema contra una usurpación de datos de identificación y autenticación (especialmente los proporcionados por el usuario U1 durante el acceso no securizado), esta relación solo se verifica además si un secreto del primer usuario U1, es decir una información PWD1 propia del primer usuario U1, se ha proporcionado al servidor AS en la segunda sesión por parte del segundo usuario U1bis. Esta información PWD1 puede ser, por ejemplo, una frase clave, una contraseña, un código personal o de un objeto asociado de forma unívoca a dicho usuario, etc. Esta información la proporciona el propio usuario en la primera sesión, o la genera y/o proporciona el servidor AS.

Más generalmente, esta relación se verifica si se establece una relación entre una información PWD1 propia del primer usuario U1 y una información PWD1bis propia del segundo usuario U1bis, pudiendo ser dicha relación:

- una relación de igualdad entre ambas informaciones PWD1 y PWD1bis;

- una relación de igualdad entre una de estas dos informaciones y una transformación (cifrado, descifrado, codificación, descodificación, hash, etc.) de la otra información;

- una relación de igualdad entre una transformación (cifrado, descifrado, codificación, descodificación, hash, etc.) de una de las informaciones y una transformación de la otra información (cifrado, descifrado, codificación, descodificación, hash, etc.).

Cualquiera que sea el método utilizado para comprobar si existe una relación entre estas dos informaciones PWD1 y PWD1bis, se pueden obtener estas informaciones de distintas maneras: bien las proporciona el usuario (es el caso por ejemplo cuando dicha información es un identificador de un usuario o cuando el usuario es quien genera su propio código), bien las genera el servidor AS (es el caso por ejemplo cuando dicha información es en forma de contraseña de un único uso).

Se puede emplear cualquier otro método que permita establecer que existe una relación entre el primero y el segundo usuario. Preferiblemente, el servidor AS definirá y verificará una relación biunívoca, de manera a garantizar que solo un usuario esté autorizado a validar operaciones solicitadas por otro usuario.

La comprobación de dicha relación permite evitar que una operación de origen fraudulento, solicitada por un pirata, sea validada a posteriori.

Finalmente, dicha relación puede servir para el servidor AS como identificador a partir del cual el servidor AS puede encontrar un juego de operaciones a validar: en este caso, la información PWD1 propia del primer usuario U1 y/o la información PWD1bis propia del segundo usuario U1bis se almacena en asociación con los datos intermedios, destinados a ser utilizados para validar operaciones definidas por el primer usuario. A continuación, durante la conexión del segundo usuario, las operaciones a validar se determinan a partir de la información PWD1bis propia del segundo usuario, con reserva de que se verifique la relación entre las informaciones PWD1 y PWD1bis.

Caso de datos compartidos por dos usuarios U1 y U2 distintos

En el caso en que los datos a modificar son datos D12 compartidos entre dos usuarios U1 y U2 distintos lógicamente (es decir identificados por el servidor AS por medio de dos identificadores ID1 e ID2 distintos), el usuario U1bis = U2 puede ser autorizado por el usuario U1 a validar operaciones solicitadas por el usuario U1 con datos compartidos D12 o viceversa.

En esta hipótesis, el espacio de memoria intermedia utilizado para las operaciones con datos compartidos es entonces un espacio EIT12 común a ambos usuarios (no representado).

Asimismo en esta hipótesis, la relación a verificar entre los usuarios U1 y U2 deberá ser una relación distinta de una simple relación de igualdad entre identificadores de usuarios (véase los ejemplos anteriores), dado que U1 y U2 son vistos como distintos por parte del servidor AS. La relación a verificar será por ejemplo que los usuarios U1 y U2 comparten un mismo secreto.

Caso de delegación de derechos de un usuario U1bis a un usuario U1

La invención puede combinarse con cualquier mecanismo de delegación de derechos de acceso. Efectivamente, la invención se aplica asimismo al caso en que un usuario U1bis delega derechos a un usuario U1 para que el usuario

U1 defina operaciones con datos DATA1 de los datos almacenados en el espacio de almacenamiento ES1. El usuario U1bis podrá, a continuación, durante la sesión altamente securizada, validar las operaciones definidas por el usuario U1. En este caso, la relación a verificar entre los usuarios U1 y U1bis deberá ser una relación distinta de una simple relación de igualdad entre identificadores de usuarios (véase los ejemplos anteriores), ya que U1 y U1bis son considerados distintos por parte del servidor AS. Además, el servidor AS deberá verificar previamente que el usuario U1bis dispone de una delegación por lo menos para ciertas operaciones y/o ciertos datos.

Con referencia a la figura 2, se describe un modo de realización del procedimiento según la invención.

En la etapa 200, un usuario U1 se conecta al servidor AS, proporcionando un código de identificación y una contraseña con objeto de su autenticación por parte del servidor AS por medio de un método de autenticación simple. En caso de identificación y autenticación conseguida, se establece una primera sesión de comunicación en modo escasamente securizado entre su terminal T y el servidor AS. El servidor AS, según el identificador ID1 del usuario conectado y las autorizaciones de acceso que tiene asociadas, ES1 muestra a dicho usuario una visión del espacio de almacenamiento ES1 para el que posee una autorización de acceso.

En la etapa 210, en caso de autenticación conseguida en la etapa 200, el usuario U1 formula una solicitud para la ejecución de por lo menos una operación de procesamiento con datos DATA1 almacenados en el espacio de almacenamiento ES1. El servidor AS almacena entonces unos datos intermedios DINT1, relativos a las operaciones solicitadas, en el espacio de memoria intermedia EIT1 del usuario U1 (figura 3a).

En la etapa 220, el usuario U1 transmite además al servidor AS una frase clave, por ejemplo “me llamo Arturo”. El servidor AS memoriza esta frase clave en el espacio de memoria intermedia EIT1 del usuario U1, con los datos intermedios DINT1.

En la etapa 230, el servidor AS muestra al usuario U1 una visión del contenido del espacio de memoria intermedia EIT1, que contiene los datos intermedios DINT1 generados por el servidor AS para la o las operaciones solicitadas y definidas por el usuario U1 en la etapa 210. Esta visión incluye la lista de operaciones solicitadas y/o los datos resultantes DATA1bis de dichas operaciones y/o los datos DATA1 a procesar mediante dichas operaciones con los códigos de operaciones eventualmente asociados.

En la etapa 240, se interrumpe la primera sesión de comunicación a petición del primer usuario U1.

En la etapa 300, un usuario U1bis se conecta al servidor AS, proporcionando su identificador, código PIN y certificación extraída de su tarjeta con microprocesador, con objeto de su autenticación por parte del servidor AS por medio de un método de autenticación fuerte. En caso de identificación y autenticación conseguidas, se establece una segunda sesión de comunicación en modo securizado entre el terminal T y el servidor AS.

En la etapa 310, el servidor AS, tras haber detectado que los usuarios U1 y U1bis son idénticos y están debidamente identificados por un mismo identificador ID1, muestra al usuario U1bis una visión del contenido del espacio de memoria intermedia EIT1 asociado a dicho identificador ID1. Esta visión incluye la lista de operaciones solicitadas y definidas por el usuario U1 en la etapa 220 y/o los datos resultantes DATA1bis de dichas operaciones y/o los datos DATA1 a procesar mediante dichas operaciones.

En la etapa 320, el usuario U1bis transmite además la frase clave ya transmitida en la etapa 220 y el servidor AS comprueba que la frase clave es la memorizada en el espacio de memoria intermedia EIT1.

En la etapa 330, el usuario U1bis solicita la validación de las operaciones de procesamiento visualizadas en la etapa 320 y memorizadas en el espacio de memoria intermedia EIT1 en asociación con la frase clave. El servidor AS ejecuta entonces dichas operaciones, por ejemplo copiando datos DATA1bis resultantes de dichas operaciones desde el espacio de memoria intermedia EIT1 hacia el espacio de almacenamiento ES1 1 asociado al usuario U1 (figura 3b).

En la etapa 340, la segunda sesión de comunicación se interrumpe a petición del usuario U1bis.

La invención se generaliza con el empleo de un modo de acceso no securizado en el que solo se requiere una identificación del primer usuario U1, en asociación con un modo de acceso securizado en el que se requiere una autenticación simple o fuerte del segundo usuario U1bis.

El segundo usuario U1bis, que se conecta en la segunda sesión y es susceptible de recibir la autorización de validar operaciones solicitadas por el primer usuario U1, es bien idéntico al primer usuario U1, bien el delegado de U1, o bien un usuario U2 que comparte datos con el usuario U1.

Al generalizar, el nivel de seguridad exigido durante la segunda sesión es siempre superior al nivel de seguridad exigido durante la primera sesión, de ahí la expresión “autenticación fuerte a posteriori” utilizada para calificar el proceso de securización que pone en práctica la invención. La seguridad se garantiza porque la confianza en las

operaciones de procesamiento definidas se otorga a posteriori, durante la validación de dichas operaciones.

Autenticación fuerte a priori

La invención prevé asimismo la puesta en práctica de una “autenticación fuerte a priori”, para la que el nivel de seguridad exigido durante la primera sesión es siempre superior al nivel de seguridad exigido durante la segunda sesión.

En este caso, el nivel de securización exige que se formule un solicitud por parte de un primer usuario U1 para autorizar a priori a un usuario U1bis a definir y/o validar y/o ejecutar operaciones con unos primeros datos, durante una sesión posterior en modo escasamente securizado (es decir sin autenticación fuerte, pero únicamente con autenticación débil), con reserva de que se verifique una relación predefinida entre el primero y el segundo usuario U1 y U1bis, siendo esta relación de misma naturaleza que la descrita en el caso de una autenticación fuerte a posteriori. En este caso, la confianza se otorga a priori durante la primera sesión, pudiendo efectuarse la definición y/o la validación y/o la ejecución de las operaciones con un nivel de confianza más débil.

Preferiblemente, la ejecución y/o la definición y/o la validación de una operación de procesamiento solo se autoriza durante la sesión posterior si se cumple una condición predeterminada, fijada por el primer usuario U1 en la primera sesión en el momento de formular la solicitud de autorización. Esta condición es, por ejemplo, que la ejecución y/o la definición y/o la validación de una operación se requiera y/o inicie durante un período definido por el primer usuario U1 en la primera sesión (por ejemplo, un día, una hora, etc.); o bien que las operaciones definidas / validadas / ejecutadas durante una sesión posterior se limiten a ciertas operaciones y/o a ciertos datos elegidos por el primer usuario U1 en la primera sesión. Esta condición pretende limitar los riesgos de violación de los datos del usuario U1.

De este modo, durante los accesos posteriores con autenticación débil, las operaciones solicitadas y, por lo tanto, los datos resultantes de estas operaciones solo se validarán, es decir que las operaciones solo se ejecutarán efectivamente, si se verifica la relación entre los dos usuarios U1 y U1bis y si se verifica la condición formulada por el primer usuario U1 durante la sesión posterior en el momento de la ejecución y/o la definición y/o la validación de una operación.

La relación a comprobar entre los dos usuarios U1 y U1bis implicará preferiblemente proporcionar, por parte del segundo usuario U1bis, una información propia del primer usuario U1 ya que, en el caso de una autenticación fuerte a priori, las consecuencias de una usurpación de identidad por parte del segundo usuario U1bis podrían ser la destrucción, por parte del pirata, de los datos del primer usuario o su falsificación. Este no es el caso en el método de identificación fuerte a posteriori, ya que el segundo usuario U1bis dispone por lo menos de la posibilidad de comprobar las operaciones solicitadas antes de validarlas.

En el caso de una autenticación fuerte a priori, igual que en caso de autenticación fuerte a posteriori, es posible que los usuarios U1 y U1bis que se conecten sucesivamente puedan ser distintos lógicamente uno de otro (por ejemplo U1bis = U2), pero que uno se beneficie de una delegación por parte del otro. En el caso de una autenticación fuerte a priori, es el usuario U1, al establecer la sesión altamente securizada, quien puede delegar derechos a otro usuario U1bis para una sesión escasamente securizada posterior.

Ejemplo de aplicación: caso de una autenticación fuerte a posteriori

La invención es aplicable, por ejemplo, al ámbito médico. En este ámbito, en Francia, la legislación impone una fuerte securización de los datos médicos y recomienda para ello que los profesionales de la salud utilicen su tarjeta CPS (Tarjeta Profesional de Salud) como medio de autenticación fuerte para acceder a dichos datos médicos. Cada vez más, los servicios médicos exigen, por lo tanto, que los datos transmitidos sean datos denominados de confianza, es decir protegidos, tanto para lectura como escritura. Sin embargo, algunos de esos mismos servicios aceptan que el acceso para lectura (incluso para escritura) se base en una autenticación simple como solución paliativa de la tarjeta CPS, dado que esta no puede utilizarse en todos los casos.

Tomemos el caso de un médico que posee su propia consulta: durante su jornada de trabajo, puede utilizar distintos servicios securizados, con su tarjeta CPS insertada permanentemente en el lector de tarjetas con microprocesador de su ordenador de trabajo. Cuando regresa a su casa, puede no llevar su tarjeta CPS, o no disponer de un lector de tarjetas con microprocesador en su ordenador personal. La única solución para acceder al servicio securizado es, en este caso, la autenticación simple, fallo de seguridad evidente para un servicio sensible.

En dicha situación, la invención permite al profesional de la salud utilizar el servicio de acceso a sus datos con una autenticación simple, y definir o simular operaciones que solo se validarán durante la próxima conexión basada en una autenticación fuerte cuando, por ejemplo, este profesional de la salud regrese a su consulta. Por lo tanto, quedará garantizada la confianza de los datos transmitidos.

Otro caso de aplicación en el ámbito de la salud afecta a las prácticas de delegación al personal de secretaría del derecho de transmisión electrónica de formularios de atención sanitaria. Para ello, el médico entrega su código

personal de identificación y su contraseña en secretaría. Por lo tanto, una persona de secretaría puede requerir la ejecución de operaciones conectándose y autenticándose mediante autenticación simple sobre la base del código y la contraseña proporcionados. La validación final, es decir el envío efectivo de los formularios de atención sanitaria, se efectúa a petición del médico durante otra conexión con autenticación fuerte del médico por medio de su tarjeta CPS, mediante la transmisión al médico de una frase clave o secreto utilizado por la secretaria.

Existen muchos otros ámbitos de aplicación de esta invención, por ejemplo los sectores bancario, militar, administración electrónica, la enseñanza, etc.

REIVINDICACIONES

1. Procedimiento de procesamiento de datos aplicado por un servidor (AS), que incluye:

- una etapa de recepción (210), en una primera sesión de comunicación establecida con dicho servidor, de una solicitud formulada por un primer usuario (U1) que define por lo menos una operación de procesamiento a ejecutar con unos primeros datos;

- una etapa de ejecución (330) de dicha operación de procesamiento con dichos primeros datos, en una segunda sesión de comunicación establecida con dicho servidor posteriormente a dicha primera sesión por un segundo usuario (U1bis),

estando destinada dicha etapa de ejecución a iniciarse con la condición, por una parte, de que el segundo usuario haya sido autenticado mediante un método de autenticación fuerte en la segunda sesión y, por otra, que se haya comprobado una relación entre el primero y el segundo usuario.

2. Procedimiento, según la reivindicación 1, en el que dicha relación se comprueba si se verifica una relación entre una primera información propia del primer usuario y una segunda información propia del segundo usuario.

3. Procedimiento según la reivindicación 1, en el que dicha relación se verifica si el segundo usuario ha delegado derechos al primer usuario.

4. Procedimiento según la reivindicación 1, en el que se verifica dicha relación si un identificador del primer usuario es idéntico a un identificador del segundo usuario.

5. Procedimiento según la reivindicación 2, en el que dicha primera, respectivamente segunda, información se proporciona a dicho servidor por parte del primero, respectivamente segundo, usuario durante dicha primera, respectivamente segunda, sesión.

6. Programa informático que incluye instrucciones lógicas para la aplicación de un procedimiento según una de las reivindicaciones 1 a 5 cuando dicho programa es ejecutado por un procesador de datos.

7. Soporte de grabación legible mediante un procesador de datos en el que se graba un programa que incluye instrucciones de código de programa para la ejecución de las etapas de un procedimiento según una de las reivindicaciones 1 a 5.

8. Dispositivo de procesamiento de datos, que incluye:

- medios para recibir (210), en una primera sesión de comunicación establecida con dicho dispositivo, una solicitud formulada por un primer usuario (U1) que define por lo menos una operación de procesamiento a ejecutar con unos primeros datos;

- medios de ejecución (330) de una operación de procesamiento con dichos primeros datos, durante una segunda sesión de comunicación establecida con dicho dispositivo posteriormente a dicha primera sesión para un segundo usuario (U1bis);

estando destinados dichos medios de ejecución a ser activados con la condición, por una parte, de que el segundo usuario haya sido autenticado mediante un método de autenticación fuerte en la segunda sesión y, por otra, que se haya verificado una relación entre el primero y el segundo usuario.

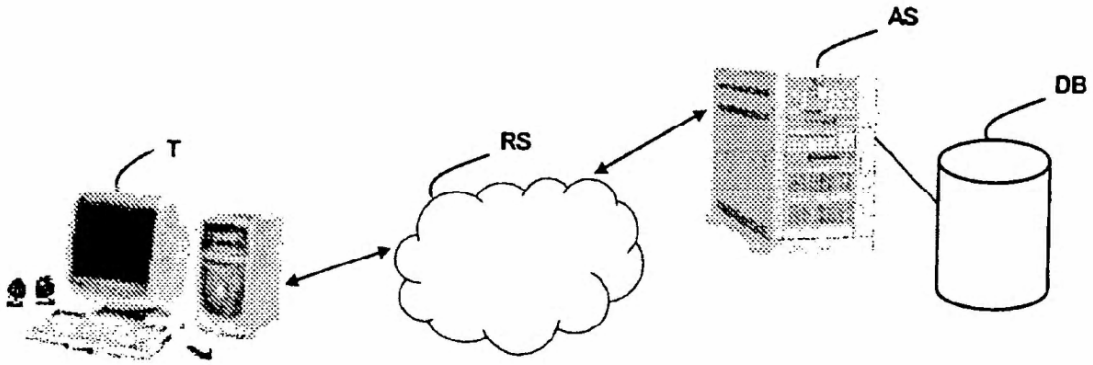

Fig. 1

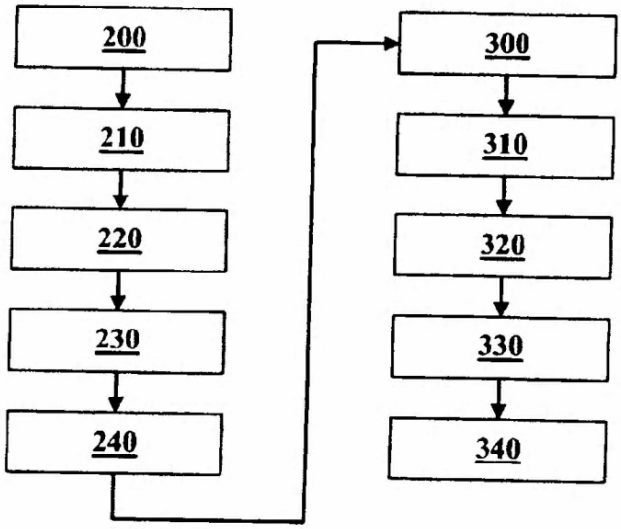

Fig. 2

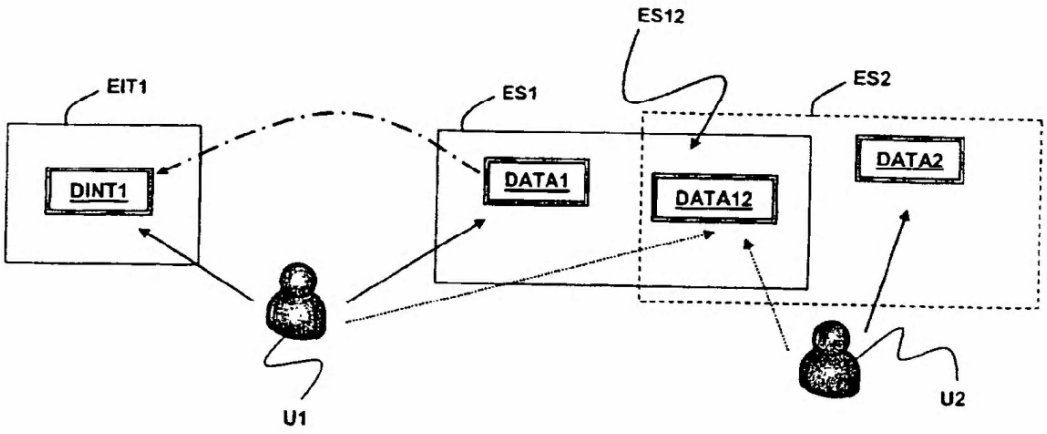
ES12
EIT1
ES1
ES2
DINT1
DATA1
DATA12
DATA2
U1
U2

Fig. 3a

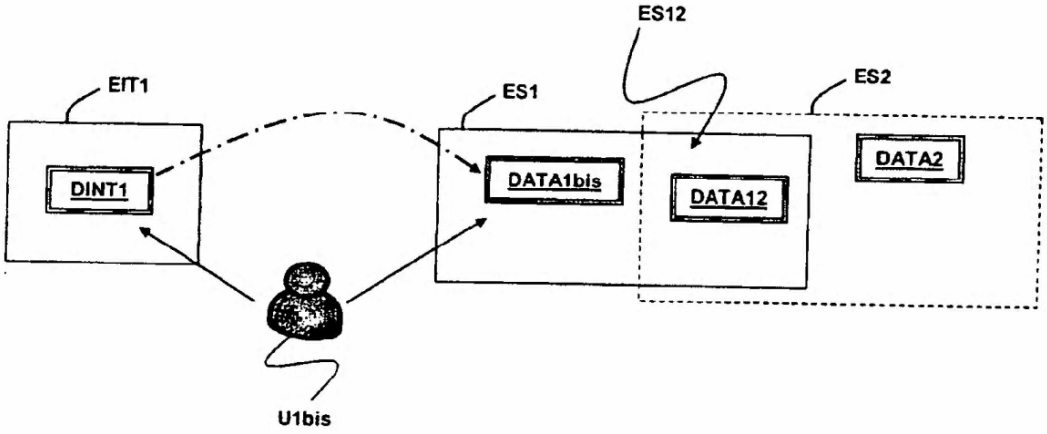
ES12
EIT1
ES1
ES2
DINT1
DATA1bis
DATA12
DATA2
U1bis

Fig. 3b