(19) OFICINA ESPAÑOLA DE PATENTES Y MARCAS

ESPAÑA

(11) Número de publicación: **2 703 426**

(51) Int. CI.:

G06F 21/31 (2013.01)

(12) TRADUCCIÓN DE PATENTE EUROPEA T3

(86) Fecha de presentación y número de la solicitud internacional: **04.02.2011 PCT/FR2011/050231**

(87) Fecha y número de publicación internacional: **25.08.2011 WO11101574**

(96) Fecha de presentación y número de la solicitud europea: **04.02.2011 E 11708064 (8)**

(97) Fecha y número de publicación de la concesión europea: **03.10.2018 EP 2537114**

(54) Título: **Procedimiento de bloqueo/desbloqueo a distancia de una máquina**

(30) Prioridad:

17.02.2010 FR 1051146

(45) Fecha de publicación y mención en BOPI de la traducción de la patente:
08.03.2019

(73) Titular/es:

EVIDIAN (100.0%)
Rue Jean Jaurès
78340 Les Clayes Sous Bois, FR

(72) Inventor/es:

DEDIEU, GÉRARD y
COSSARD, DAVID

(74) Agente/Representante:

ELZABURU, S.L.P

DESCRIPCIÓN

Procedimiento de bloqueo/desbloqueo a distancia de una máquina

Ámbito técnico de la invención

La presente invención concierne a un procedimiento de cambio de estado, bloqueado o desbloqueado, de una máquina objetivo. La invención concierne igualmente a una máquina objetivo apta para poner en práctica el procedimiento de cambio de estado.

La misma encuentra una aplicación particular, pero no limitativa, en el ámbito bancario.

Antecedente tecnológico de la invención

Un procedimiento de cambio de estado, bloqueado o desbloqueado, de una máquina objetivo, conocido por el experto en la técnica, permite bloquear la citada máquina, sea por acción del usuario de la máquina, o automáticamente cuando no se efectúe ninguna acción sobre la citada máquina a través del teclado o el ratón al cabo de un tiempo determinado.

Así, en el ámbito bancario, cuando un operador bursátil denominado habitualmente « trader » en inglés, se ausenta de su puesto de trabajo, ya sea que el mismo bloquee su máquina objetivo, o que la máquina objetivo sobre la cual opera se bloquee automáticamente al cabo de un tiempo determinado, especialmente cuando el operador bursátil se ausenta de su puesto. El bloqueo evita así a cualquier otra persona utilizar de manera ilícita esta máquina objetivo en ausencia de su usuario.

El operador bursátil lanza operaciones bursátiles por medio de la máquina objetivo. Estas operaciones bursátiles son scripts que a veces pueden durar varias horas.

Estas operaciones bursátiles dependen de datos muy sensibles que evolucionan rápidamente en el transcurso del tiempo tales como un valor en bolsa, datos económicos o políticos. Por este motivo es necesario no perder de vista la evolución en el transcurso del día de las operaciones bursátiles que han sido lanzadas. Cuando el operador bursátil se ausenta de su puesto, los datos en la pantalla de la máquina objetivo permanecen visibles así como el desarrollo de las operaciones bursátiles que han sido lanzadas.

Un inconveniente de este estado de la técnica es que cuando un operador bursátil se ausenta de su puesto, según la fluctuación de los datos sensibles anteriormente mencionados, es a veces necesario detener o modificar rápidamente las operaciones bursátiles que han sido lanzadas. Como la máquina objetivo ha sido bloqueada para evitar a cualquier otra persona utilizar fraudulentamente esta máquina objetivo, no es posible ninguna intervención sobre la máquina objetivo por un usuario de otra máquina para efectuar estas acciones sobre las operaciones bursátiles.

En el estado de la técnica es conocido el sistema xscreensaver, véase http://manpages.ubuntu.com/manpages/dapper/man_1/xscreensaver-command.1. htlm que divulga el bloqueo y el desbloqueo de una máquina a distancia.

Descripción general de la invención

La presente invención tiene por objetivo un procedimiento de cambio de estado, bloqueado o desbloqueado, de una máquina objetivo, que permita resolver los problemas que pueden sobrevenir en la citada máquina objetivo en ausencia de un usuario y especialmente cuando la citada máquina haya sido bloqueada anteriormente.

Este objetivo es conseguido por un procedimiento de cambio de estado, bloqueado o desbloqueado, de una máquina objetivo que comprende un servicio de seguridad y un módulo de gestión de sesión, comprendiendo el procedimiento las etapas de:

- recibir por el citado servicio de seguridad una petición correspondiente a una solicitud de cambio de estado de la máquina objetivo, comprendiendo la citada petición al menos una información de identificación de un usuario de una máquina fuente;
- a partir del citado servicio de seguridad, verificar si derechos de acceso a la citada máquina objetivo asociados al citado usuario de la máquina fuente autorizan un cambio de estado de la máquina objetivo por el citado usuario;
- en caso afirmativo, a partir de citado servicio de seguridad, enviar un mensaje de cambio de estado al módulo de gestión de sesión de la citada máquina objetivo y proceder al citado cambio de estado por el citado módulo de gestión de sesión.

Como se va a ver en detalle en lo que sigue, gracias a la autorización de cambio de estado de la máquina objetivo que se da a un usuario de una máquina fuente (diferente de la máquina objetivo) a través de los derechos de acceso asociados, este último podrá desbloquear a distancia la máquina objetivo (por tanto la máquina de otra persona) que

esté bloqueada, es decir que podrá desbloquear una sesión de usuario que el mismo no ha abierto. Inversamente, podrá bloquear la máquina objetivo a distancia si ésta está en un estado desbloqueado.

Según modos de realización no limitativos, el procedimiento puede comprender además una o varias de las características suplementarias entre las siguientes:

- El procedimiento comprende una etapa suplementaria de registro en una base de gestión de peticiones, de informaciones de trazabilidad correspondientes a la citada petición.

  Esto permite hacer una auditoría sobre las citadas peticiones y especialmente verificar cuál es la verdadera persona que es origen de una acción sobre la máquina objetivo.

- Los derechos de acceso dependen de parámetros de delegación de un grupo de usuarios en otro grupo de usuarios.

  Esto permite gestionar autorizaciones de delegación de derechos de acceso por un administrador de un parque de máquinas que comprende la máquina objetivo y la máquina fuente.

- Los parámetros de delegación son activables por un usuario de un grupo de usuarios.

  Esto permite activar una delegación de derechos de acceso a nivel de usuario. Este último controla entonces autorizaciones que da a usuarios de otras máquinas para acceder a su máquina en el límite de las delegaciones autorizadas por el administrador del parque de máquinas.

- A los derechos de acceso están asociados parámetros de ejecución.

  Los derechos de acceso son así configurables.

- La petición de cambio de estado es una petición TC/IP o UDP.

  Esto permite una comunicación entre dos máquinas de una misma red informática.

- Un mensaje de cambio de estado es un mensaje aplicativo definido en función del módulo de gestión de sesión de la máquina objetivo.

  Esto permite utilizar mensajes estándar existentes.

- El mensaje de cambio de estado es enviado a una inserción del módulo de gestión de sesión.

  Esto evita modificar la interfaz de usuario de gestión de sesión que está comprendida en el módulo de gestión de la máquina objetivo.

La invención concierne igualmente a una máquina objetivo que comprende un servicio de seguridad y un módulo de gestión de sesión, siendo la citada máquina objetivo apta para:

- recibir por el citado servicio de seguridad una petición correspondiente a una solicitud de cambio de estado, comprendiendo la citada petición al menos una información de identificación de un usuario de una máquina fuente;

- a partir del citado servicio de seguridad, verificar si derechos de acceso asociados al citado usuario de la máquina fuente autorizan un cambio de su estado por el citado usuario,

- en caso afirmativo, a partir del citado servicio de seguridad, enviar un mensaje de cambio de estado al módulo de gestión de sesión y proceder al citado cambio de estado por el citado módulo de gestión de sesión.

Según un modo de realización, el módulo de gestión de sesión comprende.

- una inserción apta para recibir un mensaje de cambio de estado del citado servicio de seguridad; y

- una interfaz de usuario de gestión de sesión apta para ser solicitada por la citada inserción para cambiar de estado la citada máquina objetivo.

La invención concierne igualmente a una máquina fuente apta para cooperar con una máquina objetivo según una de las características precedentes, comprendiendo la citada máquina objetivo un servicio de seguridad, siendo la citada máquina fuente apta para:

- recibir una solicitud de cambio de estado de la máquina objetivo de un usuario de la máquina fuente; y

- enviar una petición correspondiente a la citada solicitud al servicio de seguridad de la citada máquina objetivo, comprendiendo la citada petición al menos una información de identificación de un usuario de la citada máquina fuente.

La invención concierne igualmente a un sistema informático apto para efectuar un cambio de estado, bloqueado o desbloqueado, de una máquina objetivo, comprendiendo el citado sistema informático una máquina objetivo según una cualquiera de las características precedentes, y una máquina fuente según la característica precedente apta para cooperar con la citada máquina objetivo.

La invención y sus diferentes aplicaciones se comprenderán mejor con la lectura de la descripción que sigue y del examen de las figuras que la acompañan.

Breve descripción de las Figuras

Las mismas se presentan únicamente de modo indicativo y en modo alguno limitativo de la invención.

- La Fig.1 ilustra especialmente un primer organigrama simplificado de un modo de realización no limitativo de procedimiento de cambio de estado según la invención,

- La Fig. 2 ilustra especialmente un segundo organigrama simplificado del procedimiento de cambio de estado de la Fig.1, comprendiendo el citado procedimiento además una etapa suplementaria de registro de informaciones de trazabilidad de una petición;

- La Fig. 3 es una primera representación esquemática de un sistema informático que comprende una máquina objetivo y una máquina fuente, según un primer modo de realización no limitativo, siendo la citada máquina objetivo apta para poner en práctica el procedimiento de cambio de estado de las Figs.1 y 2;

- La Fig. 4 ilustra esquemáticamente intercambios de peticiones y de mensajes entre una máquina objetivo y una máquina fuente según un modo de realización no limitativo del procedimiento de la Fig. 2;

- la Fig. 5 es una segunda representación esquemática de un sistema informático que comprende una máquina objetivo y una máquina fuente, siendo la citada máquina objetivo apta para poner en práctica el procedimiento de cambio de estado de las Figs. 1 y 2.

- La Fig.6 es una tercera representación esquemática de un sistema informático que comprende una máquina objetivo y una máquina fuente, según un segundo modo de realización no limitativo, siendo la citada máquina objetivo apta para poner en práctica el procedimiento de cambio de estado de las Figs. 1 y 2.

Descripción de modos de realización de la invención

El procedimiento de cambio de estado, bloqueado o desbloqueado, de una máquina objetivo que comprende un servicio de seguridad y un módulo de gestión de sesión, se describe en un modo de realización no limitativo en la Fig. 1 y en la Fig. 2.

Se entiende por cambio de estado, bloqueado slo o desbloqueado sul, de una máquina, el hecho de desbloquear una sesión de usuario que está bloqueada o bloquear una sesión de usuario que está desbloqueada.

El procedimiento de cambio de estado es puesto en práctica por la máquina objetivo en un sistema informático SYS que comprende la citada máquina objetivo PC1 y una máquina fuente PC2 tal como está ilustrado en la Fig. 3.

Por máquina, se entiende cualquier material informático que comprenda una interfaz de usuario por la cual un usuario puede autenticarse con su identificador y su contraseña. En ejemplos no limitativos, una máquina puede ser un puesto de trabajo individual o un servidor.

Cuando un primer usuario USR1 de la máquina objetivo PC1 accede a la citada máquina, éste se conecta en una sesión de usuario propia a través de un identificador propio y de una contraseña asociada. La conexión (denominada igualmente apertura de sesión) se hace a través de una interfaz de usuario de gestión de sesión UI1 que es un componente de la interfaz de usuario (no representada) de la máquina. El identificador y la contraseña forman lo que se denomina habitualmente un « login ». Una sesión de usuario puede ser bloqueada manualmente por el primer usuario o automáticamente después de un tiempo determinado, de modo que ninguna persona pueda acceder a la máquina objetivo PC1.

En lo que sigue de la descripción, se utilizará indiferentemente el término sesión de usuario o el término sesión.

Cuando un segundo usuario USR2 de la máquina fuente PC2 quiere efectuar a distancia un cambio de estado, bloqueado o desbloqueado, de la máquina objetivo PC1 (para acceder a la misma) inicia una solicitud DDE de cambio de estado de la máquina objetivo PC1 desde la máquina fuente PC2. Lo hace por medio de una interfaz de usuario MODUI2 asociada a un módulo de bloqueo/desbloqueo MOD2 de la máquina fuente PC2, tal como está ilustrado en la Fig. 3.

En un ejemplo no limitativo, la interfaz de usuario MODUI2 está compuesta de un icono en una barra de tareas en la pantalla de la máquina PC2 y propone:

- una lista de usuarios (entre los cuales el primer usuario USR1) que han activado los derechos de acceso a sus máquinas asociadas al segundo usuario USR2,

- y, después de que el segundo usuario USR2 haya elegido el primer usuario USR1, una lista de máquinas del segundo usuario USR2 de las cuales el segundo usuario tiene efectivamente los derechos de acceso.

Así, la máquina fuente PC2 recibe la solicitud DDE de cambio de estado de la máquina objetivo PC1 del usuario USR2 de la máquina fuente PC2, tal como está ilustrado en la Fig. 2 (etapa RX_DDE (PC2) indicada como etapa previa 0) en las Figs. 1, 2 y 4.

En un modo de realización no limitativo, a solicitud de la interfaz de usuario MODUI2, la solicitud DDE de cambio de estado de la máquina objetivo PC1 es envida al módulo de bloqueo/desbloqueo MOD2 de la máquina fuente PC2.

A continuación, la citada máquina fuente PC2 envía al citado servicio de seguridad SES1 de la citada máquina objetivo PC1 una petición RQ correspondiente a la citada solicitud DDE, comprendiendo la ciada petición RQ al menos una información de identificación ID del usuario USR2 de la máquina fuente PC2 (etapa TX_RQ (DDE, ID, SES1) indicada como etapa previa 0') en las Figs. 1, 2 y 4.

En un modo de realización no limitativo, el módulo de bloqueo/desbloqueo MOD2 de la máquina fuente PC2 envía la citada petición RQ.

En modos de realización no limitativos, la petición RQ de cambio de estado es una petición TCP/IP (« Transmission Control Protocol/Internet Protocol » en inglés) o UDP (« User Datagram Protocol » en inglés). En este último caso, las peticiones son denominadas datagramas. El protocolo de comunicación UDP es un protocolo simple que permite enviar peticiones a otra máquina sin solicitud de comunicación previa. Naturalmente, pueden utilizarse otros protocolos de comunicación que permitan un envío de petición entre dos máquinas.

En este momento, el procedimiento de cambio de estado es puesto en práctica.

El citado procedimiento comprende las etapas siguientes tales como las ilustradas en la Fig. 1 y en la Fig. 2:

- recibir por el citado servicio de seguridad SES1 una petición RQ correspondiente a una solicitud DDE de cambio de estado de la máquina objetivo PC1, comprendiendo la citada petición RQ al menos una información de identificación ID de un usuario USR2 de una máquina fuente PC2 (etapa RX_RQ (DDE, ID, SES1));

- a partir del citado servicio de seguridad SES1, verificar si derechos de acceso Rgt a la citada máquina objetivo PC1 asociados al citado usuario USR2 de la máquina fuente PC2 autorizan un cambio de estado de la máquina objetivo PC1 por el citado usuario USR2 (etapa VERIF_RGT (USR2));

- en caso afirmativo, a partir del citado servicio de seguridad SES1, enviar un mensaje de cambio de estado MSG al módulo de gestión de sesión M1 de la citada máquina objetivo PC1 (etapa TX(MSG)) y proceder al citado cambio de estado slo/sul por el citado módulo de gestión de sesión M1 (etapa CHG(FCTd(sul), FCTv(sol))).

En un modo de realización no limitativo, en caso negativo, el procedimiento de cambio de estado comporte una etapa suplementaria de enviar a partir del citado servicio de seguridad SES1 un mensaje de error MSG_NOK para advertir al segundo usuario USR2 de que el mismo no tiene los derechos para bloquear/desbloquear la máquina objetivo PC1 (etapa TX(MSG_NOK)).

Según un modo de realización no limitativo, el procedimiento comprende además una etapa suplementaria de registro, en una base de gestión de peticiones BDRQ, de informaciones de trazabilidad H, D, IDU, GUI correspondiente a la citada petición RQ (etapa SAV_BDRQ (H, D, IDU, GUI) ilustrada en la Fig. 2).

En lo que sigue de la descripción, en el modo de realización no limitativo del procedimiento descrito, el procedimiento comprende estas etapas suplementarias.

Las etapas del procedimiento de cambio de estado se describen a continuación en detalle refiriéndose a las Figs. 2, 3 y 4.

En el ejemplo que sigue, la máquina objetivo PC1 se encuentra en un estado bloqueado slo.

Se recuerda que cuando una máquina está bloqueada, la sesión de usuario está bloqueada. Esto significa que no es posible ninguna acción de usuario, excepto a través del teclado de la máquina objetivo PC1 por el cual la sola acción posible es la reactivación de la sesión de usuario introduciendo el identificador de usuario y la contraseña asociada al primer usuario USR1

Se observará que la máquina fuente PC2 comprende un módulo de bloqueo/desbloqueo MOD2, una interfaz de usuario MODUI2 asociada y una interfaz de usuario de gestión UI2, y la máquina objetivo PC1 comprende una interfaz de usuario de gestión de sesión UI1, estando esta última situada en un módulo de gestión de sesión MI, tal como está ilustrado en la Fig. 3.

En una primera etapa 1), el citado servicio de seguridad SES1 recibe una petición RQ correspondiente a una solicitud DDE de cambio de estado de la máquina objetivo PC1, comprendiendo la citada petición RQ al menos una información de identificación ID de un usuario USR2 de una máquina fuente PC2.

Esta información de identificación ID permite identificar el autor de la petición RQ, o sea en este caso el segundo usuario USR2 y por consiguiente los derechos de acceso asociados al citado usuario USR2 utilizados en la etapa siguiente. En un ejemplo no limitativo, esta información de identificación ID es un identificador único asociado al usuario (denominado habitualmente en inglés « Global Unique Identifier »).

En una segunda etapa 2), el servicio de seguridad SES1 verifica si derechos de acceso Rgt a la citada máquina objetivo PC1 asociados al citado usuario USR2 de la máquina fuente PC2 autorizan un cambio de estado de la máquina objetivo PC1 por el citado usuario USR2.

En un modo de realización no limitativo, los derechos de acceso Rgt dependen de parámetros de delegación Dlg de un grupo de usuario G1 en otro grupo de usuarios G2.

Se observará que estos parámetros son definidos por un administrador ADM que gestiona un parque de máquinas en el cual se encuentran la máquina objetivo PC1 y la máquina fuente PC2.

Así, en un ejemplo no limitativo, un parámetro de delegación Dlg puede estipular que un primer grupo G1 de usuarios, denominado grupo delegante, (comprendiendo el citado grupo el primer usuario USR1) tiene el derecho de autorizar a un segundo grupo G2 de usuarios, denominado grupo delegatario, (comprendiendo el citado grupo el segundo usuario USR2) a acceder a las máquinas PC que los mismos utilizan. Este derecho de autorización se denomina una delegación. Estos parámetros de delegación Dlg permiten así posicionar las delegaciones a un nivel de administrador.

Se observará que, naturalmente, un grupo G puede contener un solo usuario.

En un modo de realización no limitativo, los parámetros de delegación Dlg son activables por un usuario USR de un grupo de usuarios G1.

Así, las delegaciones pueden ser activadas por cada usuario USR del primer grupo G1. Así, los derechos de acceso asociados a los usuarios delegatarios, en este caso el derecho de acceso a la máquina objetivo PC1 por el segundo usuario USR2, han ido activados por el primer usuario USR1, el delegante. La activación de los parámetros de delegación se hace por tanto a nivel de usuario.

En un modo de realización no limitativo, a los derechos de acceso Rgt están asociados parámetros de ejecución T.

Estos parámetros de ejecución permiten especializar los derechos de acceso Rgt a un nivel de usuario. En ejemplos no limitativos:

- un primer parámetro de ejecución T1 puede ser un tiempo de duración de activación de la delegación. Así, en un ejemplo no limitativo, el primer usuario USR1 puede autorizar al segundo usuario USR2 a acceder a la máquina objetivo PC1 únicamente durante un tiempo determinado. La activación es así temporal. En otro ejemplo, la activación puede ser permanente.

- un segundo parámetro de ejecución T2 puede determinar las acciones autorizadas por los derechos de acceso Rgt. Así, por ejemplo, el segundo usuario USR2 puede tener derechos de acceso a la máquina objetivo PC1 pero únicamente para desbloquear/bloquear la citada máquina objetivo y detener o modificar una operación bursátil, pero no tendrá los derechos para lanzar otra operación bursátil.

- un tercer parámetro de ejecución T3 puede determinar el número de veces que un usuario tiene el derecho a acceder a una máquina objetivo Esto evita los accesos inoportunos por parte de un usuario que tiene derechos de acceso a una máquina.

Se observará que estos parámetros de delegación Dlg, su activación y los parámetros de ejecución T son salvaguardados en un sistema de referencia REF de derechos de acceso al sistema informático SYS, tal como está ilustrado en la Fig. 3. En un ejemplo no limitativo, el sistema de referencia es un anuario LDAP.

El servicio de seguridad SES1 tiene acceso a este sistema de referencia REF y verifica así los derechos de acceso Rgt verificando por una parte el posicionamiento de los parámetros de delegación Dlg (efectuado por el administrador ADM) y por otra su activación.

Naturalmente, los parámetros de ejecución T son verificados al mismo tiempo.

Esta doble verificación (parámetros de delegación y activación) permite al servicio de seguridad SES1 ser autónomo. No hay necesidad de otra máquina de control para que el mensaje de cambio de estado MSG que sigue a continuación sea enviado.

Se observará que el servicio de seguridad SES1 es una tarea de fondo que funciona de modo independiente de una sesión de usuario, es decir incluso en ausencia de una sesión de usuario.

Así, el hecho de que el servicio de seguridad SES1 sea autónomo del módulo de usuario de gestión de sesión M1 (que gestiona las sesiones de usuarios) permite evitar que el citado servicio de seguridad SES1 deje de funcionar cuando el citado módulo de usuario de gestión de sesión M1 no esté activo como es el caso con ciertos sistemas de explotación (no representados en las figuras), tal como por ejemplo Windows Vista™ en los cuales se apoya el citado módulo M1.

Por otra parte, ese observará que de manera general, los derechos de un usuario sobre una máquina están limitados a cierto entorno y por tanto a ciertas acciones.

Como el servicio de seguridad SES1 es independiente de la sesión de usuario, la interfaz de usuario de gestión de sesión UI1 no tiene los mismos derechos que el citado servicio de seguridad SES1 y por tanto no tiene acceso a las acciones ejecutadas por el servicio de seguridad SES1. Así, esta independencia evita a un usuario tener acceso de manera ilícita a los parámetros de delegación Dlg y modificar de modo inoportuno el posicionamiento de sus derechos de acceso Rgt por ejemplo.

En una tercera etapa 3), en el caso afirmativo (cuando el segundo usuario USR2 tiene los derechos de acceso a la máquina objetivo PC1), el citado servicio de seguridad SES1 envía un mensaje de cambio de estado MSG al módulo de gestión de sesión M1 de la citada máquina objetivo PC1.

Naturalmente, en el caso negativo (etapa 3') (cuando el segundo usuario USR2 no tiene ningún derecho de acceso a la máquina objetivo PC1), el citado servicio de seguridad SES1 envía un mensaje de error MSG_NOK para advertir al usuario de que el mismo no tiene los derechos para bloquear/desbloquear la máquina objetivo PC1.

Se observará que un mensaje de cambio de estado MSG es un mensaje aplicativo que es definido en función del módulo de gestión de sesión M1 de la máquina objetivo PC1 y de modo más particular en función de la interfaz de usuario de gestión de sesión UI1. Es lo mismo en un mensaje de error MSG_NOK.

Así, por ejemplo, en el caso de una interfaz de usuario de gestión de sesión Windows™, un mensaje de cambio de estado es una notificación generada por Windows. En otro ejemplo, en el caso de una interfaz de usuario de gestión de sesión Linux™, un mensaje de cambio de estado es un acontecimiento generado por Linux™.

Se observará por otra parte que en el caso en que el módulo de usuario de gestión de sesión M1 no esté activo (como se explicó anteriormente según los sistemas de explotación), la recepción de un mensaje aplicativo MSG, MSG_NOK le estimula y le activa de nuevo.

En un primer modo de realización no limitativo, el mensaje de cambio de estado MSG es enviado directamente a la interfaz de usuario de gestión de sesión UI1 del módulo de gestión de sesión M1, como está ilustrado en la Fig. 4 por una flecha de trazo completo (etapa TX (MSG) o TX (MSG_NOK)). A la recepción de este mensaje MSG, la citada interfaz UI1 llama a una función de desbloqueo de bajo nivel FCTd (sul) del sistema de explotación (no representado) de la citada máquina objetivo PC1.

En un segundo modo de realización no limitativo, el mensaje de cambio de estado MSG es enviado a una inserción PLGN1 del módulo de gestión de sesión M1, tal como está ilustrado en la Fig. 4 por una flecha en forma de trazos (etapa TX (MSG) o TX (MSG_NOK). La inserción PLGN1, denominada habitualmente « Plugin » en inglés, solicita entonces a la interfaz de usuario de gestión de sesión UI1 del módulo de gestión de sesión M1. En esta solicitación, la interfaz UL1 llama a la función de desbloqueo de bajo nivel FCTd(sul) del sistema de explotación (no representado) de la citada máquina objetivo PC1.

La utilización de una inserción PLGN1 evita modificar la interfaz de usuario de gestión de sesión existente en una máquina para integrar una función de recepción del mensaje de cambio de estado MSG o reemplazarla por una nueva interfaz de usuario de gestión de sesión que integra la función de recepción del mensaje de cambio de estado MSG, como es el caso en el primer modo de realización anterior.

En un ejemplo no limitativo, esta función de desbloqueo FCTd(sul) se encuentra en una biblioteca de enlaces dinámica. Según los tipos de sistemas de explotación, esta biblioteca tendrá una extensión diferente (por ejemplo dll « dynamic link library » en inglés, so de « shared objet » en inglés, dylib de « dynamic library » en inglés; .a de « archive en inglés); sl de « shared library » en inglés; sa de « archive » en inglés). Siendo tales bibliotecas conocidas por el experto en la técnica, las mismas no serán descritas aquí más en detalle.

En otro ejemplo no limitativo, esta función de desbloqueo FCTd(sul) es una función binaria. En este caso, contrariamente a las bibliotecas de enlaces dinámicas, la misma necesita una recopilación del módulo de usuario de gestión de sesión M1.

En una cuarta etapa 4), el citado módulo de gestión de sesión M1 procede al citado cambio de estado slo/sul (cuando la etapa 3 ha sido efectuada). En particular, este cambio de estado es efectuado por la interfaz de usuario de gestión de sesión UI1 con la función de bajo nivel FCTd(sul) como se explicó anteriormente.

Así, en el ejemplo considerado, después del cambio de estado, la máquina objetivo PC1 es desbloqueada (estado desbloqueado sul).

De esta manera, el segundo usuario USR2 ha podido acceder a la máquina objetivo PC1 sin tener necesidad del « login » (identificador de usuario más contraseña) del primer usuario USR1. Gracias a sus derechos de acceso Rgt a la máquina objetivo PC1, el mismo ha podido desbloquear la sesión de usuario que había sido abierta y después bloqueada por el primer usuario USR1. El segundo usuario USR2 ha podido tomar el control en esta sesión.

El segundo usuario USR2 puede a continuación desplazarse al emplazamiento de esta máquina objetivo PC1y efectuar cualquier acción necesaria en la citada máquina objetivo PC1 (a través por ejemplo del teclado, el ratón o de la pantalla de la citada máquina objetivo), y especialmente detener una operación bursátil en el marco de la aplicación descrita.

Se observará que a continuación de este desbloqueo y esta intervención sobre una operación bursátil lanzada a partir de la máquina objetivo PC1, el segundo usuario USR2 puede entonces volver a su lugar y, si el mismo no ha bloqueado la sesión en PC1, bloquear a partir de su máquina fuente PC2 esta sesión de usuario en la máquina objetivo PC1 (abierta por el primer usuario USR1) que el mismo ha desbloqueado. Se recurre entonces a una función de bajo nivel de bloqueo FCTv(slo).

En una quinta etapa 5), se registran en una base de gestión de peticiones BDRQ informaciones de trazabilidad H, D, IDU, GUI correspondiente a la citada petición RQ.

En un modo de realización, no limitativo, el registro es efectuado por el servicio de seguridad SES1 de la máquina objetivo PC1.

Se observará que esta quinta etapa puede efectuarse en cualquier momento a partir de la etapa de recepción de la petición (sea en paralelo, o después).

Se observará que la base de gestión de peticiones BDRQ es gestionada por el administrador ADM del sistema informático SYS.

En ejemplos no limitativos, estas informaciones de trazabilidad pueden comprender:

- el autor IDU de la petición RQ;

- datos de identificación GUI de la máquina objetivo (nombre, dirección IP, identificador único denominado habitualmente en inglés « Global Unique Identifier »)

- informaciones temporales que comprenden:

- la fecha D a la cual ha sido lanzada la petición; y

- la hora H a la cual ha sido lanzada la petición.

Las informaciones temporales, denominadas igualmente estampilla temporal, son denominadas habitualmente en inglés « timestamp»).

Así, estas informaciones de trazabilidad permiten al administrador ADM tener un diario de peticiones RQ lanzadas en una máquina dada y especialmente conocer el usuario real que era responsable de la citada máquina en un instante dado y por tanto quien ha lanzado tal acción en la citada máquina en tal fecha y en tal hora.

Así, el procedimiento de cambio de estado permite pasar de un estado bloqueado aun estado desbloqueado o viceversa por una petición distante RQ. El mismo ofrece una funcionalidad de desbloqueo/bloqueo cliente-servidor a distancia, siendo el cliente la máquina fuente PC2 que invoca al servicio de seguridad SES1 de la máquina objetivo PC1.

El mismo permite una toma del control de una sesión de usuario por un usuario diferente del que ha abierto la citada sesión.

El procedimiento de cambio de estado es puesto en práctica por una máquina objetivo PC1 que comprende un servicio de seguridad SES1 y un módulo de gestión de sesión M1.

Un sistema informático SYS apto para efectuar un cambio de estado bloqueado slo o desbloqueado sul de una máquina objetivo PC1 según un primer modo de realización no limitativo está ilustrado en la Fig. 3 y en la Fig. 5. El mismo comprende la citada máquina objetivo PC1 y una máquina fuente PC2 apta para cooperar con la citada máquina objetivo PC1.

La citada máquina objetivo PC1 es apta para:

- recibir por el citado servicio de seguridad SES1 una petición RQ correspondiente a una solicitud DDE de cambio de estado de la máquina objetivo PC1, comprendiendo la citada petición RQ al menos una información de identificación ID de un usuario USR2 de una máquina fuente PC2,
- a partir del citado servicio de seguridad SES1, verificar si derechos de acceso Rgt asociados al citado usuario USR2 de la máquina fuente PC2 autorizan un cambio de su estado por el citado usuario USR2,
- en caso afirmativo, a partir del citado servicio de seguridad SES1, enviar un mensaje de cambio de estado MSG al módulo de gestión de sesión M1 y proceder al citado cambio de estado slo/sul por el citado módulo de gestión de sesión M1.

En un modo de realización no limitativo, el módulo de gestión de sesión M1 (denominado igualmente módulo de gestión de sesión objetivo) comprende:

- una inserción PLGN1 (denominada igualmente inserción objetivo) apta para recibir un mensaje de cambio de estado MSG del citado servicio de seguridad SES1; y

- una interfaz de usuario de gestión de sesión UI1 apta para ser solicitada por la citada inserción para cambiar de estado la citada máquina objetivo PC1.

La citada máquina fuente PC2 es apta para cooperar con la citada máquina objetivo PC1 que comprende un servicio de seguridad SES1, siendo la citada máquina fuente PC2 apta para:

- recibir una solicitud DDE de cambio de estado de la máquina objetivo PC1 de un usuario USR2 de la máquina fuente PC2; y
- enviar una petición RQ correspondiente a la citada solicitud DDE al servicio de seguridad SES1 de la citada máquina objetivo PC1, comprendiendo la citada petición RQ al menos una información de identificación ID de un usuario USR2 de la citada máquina fuente PC2.

Naturalmente, la descripción no está limitada a la aplicación, a los modos de realización y a los ejemplos anteriormente descritos.

- Así, las mismas aplicaciones anteriormente descritas para el ejemplo no limitativo de una máquina objetivo PC1 que se encuentran en un estado bloqueado slo anteriormente por el primer usuario USR1 se aplican en el caso de una máquina objetivo PC1 que se encuentra en un estado desbloqueado sul anteriormente por el primer usuario USR1. Se recurrirá en este caso a una función de bajo nivel de bloqueo FCTv(sol) para bloquear la citada máquina objetivo PC1.
- Así, en un modo de realización no limitativo, las delegaciones pueden ser activadas por el administrador ADM en lugar de un usuario de un grupo autorizado.
- Así, en un primer modo de realización no limitativo, la máquina fuente PC2 comprende igualmente un servicio de seguridad SES 2, denominado servicio de seguridad fuente, (en lugar de un programa específico tal como el módulo de desbloqueo/bloqueo MOD2) que es apto para:
  - recibir una solicitud DDE de cambio de estado de la máquina objetivo PC1 del segundo usuario USR2,
  - enviar una petición RQ correspondiente a la citada solicitud DDE al citado servicio de seguridad SES1 de la máquina objetivo PC1, comprendiendo la citada petición RQ al menos una información de identificación ID del segundo usuario USR2 de la máquina fuente PC2.

Esto evita modificar la interfaz de usuario de gestión de sesión UI2 de la máquina fuente PC2 para integrar estas dos funciones (recepción de la solicitud DDE y envío de una petición RQ correspondiente).

- Así, en un segundo modo de realización no limitativo, una inserción PLGN2 (denominada inserción fuente) está asociada a la interfaz de usuario de gestión de sesión UI2 de la máquina fuente PC2 (en lugar de un programa específico tal como el módulo de desbloqueo/bloqueo MOD2), siendo la citada inserción PLGN2 apta para recibir:
  - una solicitud DDE de cambio de estado de la máquina objetivo PC1 del segundo usuario USR2,
  - enviar una petición RQ correspondiente a la citada solicitud DDE al citado servicio de seguridad SES1 de la máquina objetivo PC1, comprendiendo la citada petición RQ al menos una información de identificación ID del segundo usuario USR2 de la máquina fuente PC2.

Esto evita modificar la interfaz de usuario de gestión de sesión UI2 de la máquina fuente PC2 para integrar estas dos funciones (recepción de la solicitud DDE y envío de una petición RQ correspondiente).

Naturalmente, los dos modos de realización (servicio de seguridad SES2 y PLGN2) pueden ser combinados entre sí tal como está ilustrado en la Fig. 6.

En este caso, la inserción fuente PLGN2 es apta para efectuar la primera función de recepción de una solicitud DDE, mientras que el servicio de seguridad fuente SES2 es apto para efectuar la segunda función de envío de una petición RQ correspondiente. La inserción fuente PLGN2 y el servicio de seguridad fuente SES2 forman un módulo de usuario de gestión de sesión fuente M2.

- Así, en un modo de realización no limitativo, el envío de una petición RQ puede efectuarse por un protocolo de comunicación distinto del TCP/IP o UDP. Puede ser utilizado cualquier protocolo de comunicación que permita un intercambio de datos en una red informática entre varias máquinas.
- Así, en un modo de realización no limitativo, durante la activación de los derechos de acceso Rgt por el primer usuario URS1 que autoriza al segundo usuario USR2 a acceder a la máquina objetivo PC1, se puede enviar un mensaje aplicativo de aceptación a la máquina fuente PC2 para que el segundo usuario USR2 acepte la citada delegación. Este mensaje es por ejemplo una caja de diálogo denominada habitualmente « pop-up » en inglés.
- Así, en un modo de realización no limitativo, se puede restringir la autorización de delegación asociada al segundo usuario USR2 a un subconjunto de máquinas del primer usuario USR1.
- Así, el procedimiento descrito puede ser utilizado en aplicaciones distintas a la descrita en el ámbito bancario. Por ejemplo el mismo puede aplicarse en el marco de una supervisión:
    - de una central nuclear,
    - de una red telefónica,
    - de una red ferroviaria,
    - en una torre de control
    - en un parque de ascensores, etc…

y de manera general en cualquier aplicación que necesite una supervisión particular en una pantalla de una máquina objetivo que pueda necesitar una intervención rápida por parte de un operador en una máquina objetivo que no sea la máquina que el mismo utiliza.

Así, la invención descrita presenta especialmente las ventajas siguientes:

- es simple de poner en práctica,
- permite cambiar a distancia el estado de una máquina por un usuario que no es el usuario de la citada máquina,
- es segura debido al servicio de seguridad objetivo SES1 que se encuentra al exterior del módulo de usuario de gestión de sesión objetivo M1 y que por tanto es independiente de este último;
- permite acceder a una máquina objetivo tomando el control de la sesión de usuario ya existente en la citada máquina objetivo y por una persona que no es usuaria de la máquina objetivo y por tanto que es diferente del usuario que anteriormente ha bloqueado/desbloqueado la sesión de usuario. Así, una misma sesión de usuario puede ser abierta y bloqueada por un usuario, pero desbloqueada por una persona diferente (o viceversa desbloqueada por un usuario pero bloqueada por una persona no usuaria diferente),
- permite hacer una auditoría de las peticiones y especialmente en lo que concierne a acciones lanzadas en una máquina gracias al diario de las peticiones y así identificar el verdadero autor de las acciones efectuadas en una máquina;
- permite tener dos niveles de acceso (un primer nivel de administrador con el posicionamiento de las delegaciones, un segundo nivel de usuario con la activación de las citadas delegaciones) para definir los derechos de acceso a una máquina objetivo asociados a una persona que no es el usuario de la citada máquina objetivo. Así, esto permite tener un doble control de los citados derechos de acceso y por tanto un nivel de control elevado;
- permite tener derechos de acceso configurables gracias a los parámetros de ejecución y así particularizar ciertos de estos derechos de acceso si es necesario,
- evita dar un login a un usuario no propietario del citado login para desbloquear/bloquear la máquina del propietario del login, lo que permite guardar la confidencialidad de citado login; y
- permite desbloquear una sesión de usuario en una máquina objetivo guardando la identidad del usuario (el primer usuario USR1 en el ejemplo considerado) en el origen de la sesión (es decir que la ha abierto) sin utilizar el login de otra persona no usuaria de la citada máquina objetivo (el segundo usuario USR2 en el ejemplo considerado).

REIVINDICACIONES

1. Procedimiento de cambio de estado, bloqueado (slo) o desbloqueado (sul), de una máquina objetivo (PC1) que comprende un servicio de seguridad (SES1), un módulo de gestión de sesión (M1), que pone en práctica una sesión para un primer usuario (USR1), comprendiendo el procedimiento las etapas de:

- recibir por el citado servicio de seguridad (SES1) una petición (RQ) correspondiente a una solicitud (DDE) de cambio de estado de la máquina objetivo (PC1), comprendiendo la citada petición (RQ) al menos una información de identificación (ID) de un segundo usuario (USR2) de una máquina fuente (PC2);

- a partir del citado servicio de seguridad (SES1), verificar si derechos de acceso (Rgt) a la citada máquina objetivo (PC1) asociados al citado segundo usuario (USR2) de la máquina fuente (PC2) autorizan un cambio de estado de la máquina objetivo (PC1) por el citado segundo usuario (USR2);

- en caso afirmativo, a partir de citado servicio de seguridad (SES1), enviar un mensaje de cambio de estado (MSG) al módulo de gestión de sesión (M1) de la citada máquina objetivo (PC1) y proceder al citado cambio de estado (slo/sul) es decir, el bloqueo o desbloqueo de la citada máquina objetivo, por el citado módulo de gestión de sesión (M1).

2. Procedimiento de cambio de estado según la reivindicación precedente, según el cual el mismo comprende una etapa suplementaria de registro, en un base de gestión de peticiones (BDRQ), de informaciones de trazabilidad (H, D, IDU, GUI) correspondientes a la citada petición (RQ).

3. Procedimiento de cambio de estado según una cualquiera de las reivindicaciones precedentes, según el cual los derechos de acceso (Rgt) dependen de parámetros de delegación (Dlg) de un grupo de usuarios (G1) en otro grupo de usuarios (G2).

4. Procedimiento de cambio de estado según la reivindicación precedente, según el cual los parámetros de delegación (Dlg) son activables por un usuario (U1) de un grupo de usuario (G1).

5. Procedimiento de cambio de estado según una cualquiera de las reivindicaciones precedentes, según el cual parámetros de ejecución (T) están asociados a los derechos de acceso (Rgt).

6. Procedimiento de cambio de estado según una cualquiera de las reivindicaciones precedentes, según el cual la petición (RQ) de cambio de estado es una petición TCP/IP o UDP.

7. Procedimiento de cambio de estado según una cualquiera de las reivindicaciones precedentes, según el cual un mensaje de cambio de estado (MSG) es un mensaje aplicativo definido en función del módulo de gestión de sesión (M1) de la máquina objetivo (PC1).

8. Procedimiento de cambio de estado según una cualquiera de las reivindicaciones precedentes, según el cual el mensaje de cambio de estado (MSG) es enviado a una inserción (PLGN1) del módulo de gestión de sesión (M1).

9. Máquina objetivo (PC1) que comprende un servicio de seguridad (SES1) y un módulo de gestión de sesión (M1), siendo la citada máquina objetivo (PC1) apta para ejecutar el procedimiento definido por la reivindicación 1.

10. Máquina objetivo (PC1) según la reivindicación precedente, según la cual el módulo de gestión de sesión (M1) comprende:

- una inserción (PLGN1) apta para recibir un mensaje de cambio de estado (MSG) del citado servicio de seguridad (SES1); y

- una interfaz de usuario de gestión de sesión (UI1) apta para ser solicitada por la citada inserción (PLGN1) para cambiar de estado la citada máquina objetivo (PC1).

11. Máquina fuente (PC2) apta para cooperar con una máquina objetivo (PC1) según la reivindicación 9 o la reivindicación 10, comprendiendo la citada máquina objetivo un servicio de seguridad (SES1), siendo la citada máquina fuente (PC2) apta para:

- recibir una solicitud (DDE) de cambio de estado de la máquina objetivo (PC1) de un usuario (USR2) de la máquina fuente (PC2), y

- enviar una petición (RQ) correspondiente a la citada solicitud (DDE) al servicio de seguridad (SES1) de la citada máquina objetivo (PC1), comprendiendo la citada petición (RQ) al menos una información de identificación (ID) de un usuario (USR2) de la citada máquina fuente (PC2).

12. Sistema informático (SYS) apto para efectuar un cambio de estado, bloqueado (slo) o desbloqueado (sul), de una máquina objetivo (PC1), comprendiendo el citado sistema informático (SYS) una máquina objetivo (PC1) según una

cualquiera de las reivindicaciones 9 o 10, y una máquina fuente (PC2) según la reivindicación 11 apta para cooperar con la citada máquina objetivo (PC1).

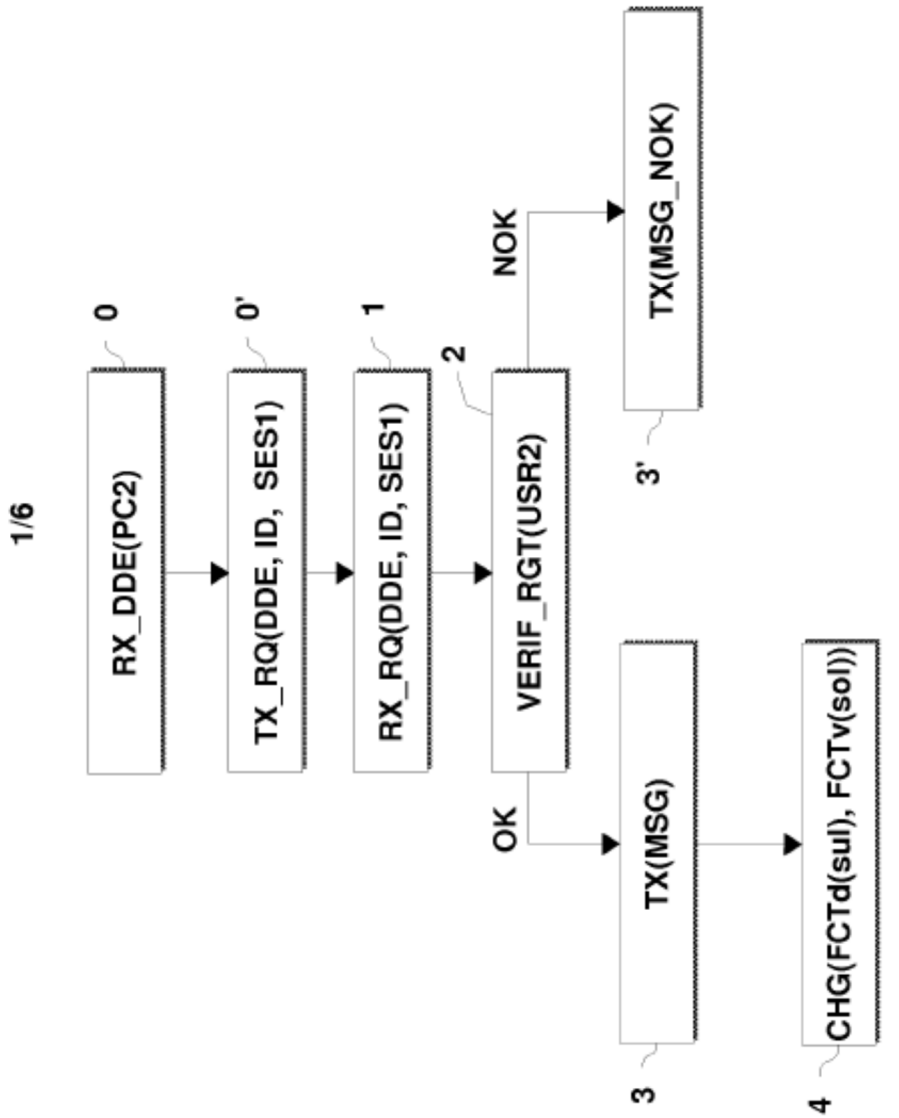
1/6
RX_DDE(PC2)
0
TX_RQ(DDE, ID, SES1)
0'
RX_RQ(DDE, ID, SES1)
1
VERIF_RGT(USR2)
2
NOK
TX(MSG_NOK)
3'
OK
TX(MSG)
3
CHG(FCTd(sul), FCTv(sol))
4

FIG. 1

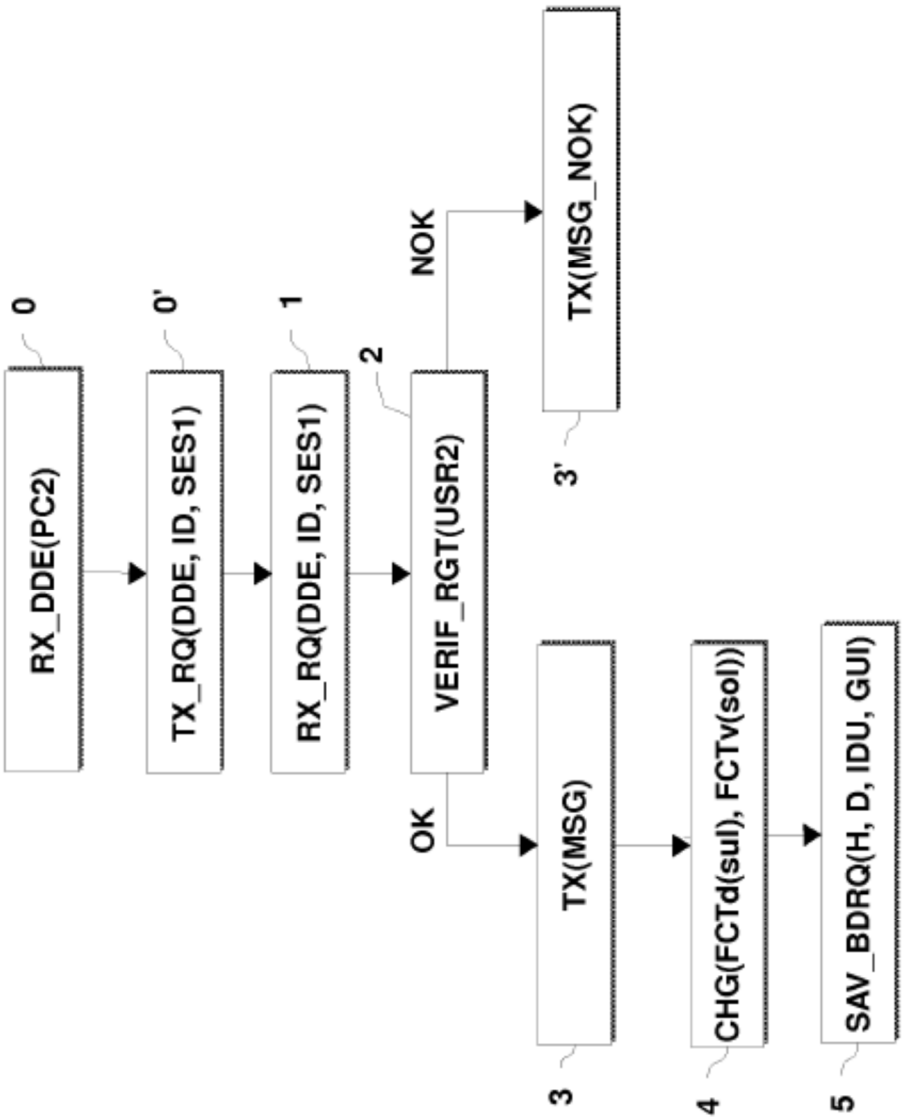
2/6
RX_DDE(PC2)
0
TX_RQ(DDE, ID, SES1)
0'
RX_RQ(DDE, ID, SES1)
1
VERIF_RGT(USR2)
2
NOK
TX(MSG_NOK)
3'
OK
TX(MSG)
3
CHG(FCTd(sul), FCTv(sol))
4
SAV_BDRQ(H, D, IDU, GUI)
5

FIG. 2

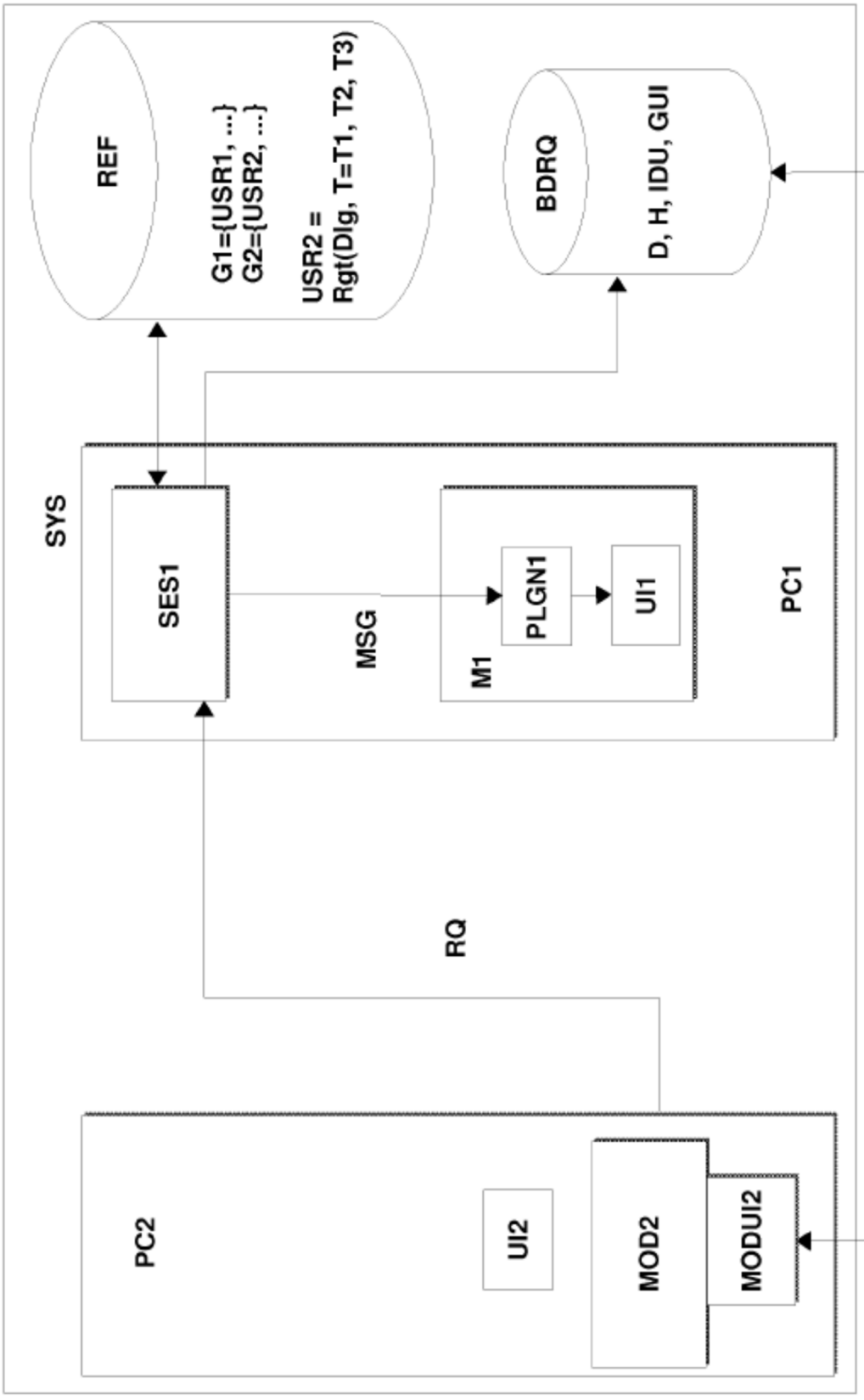
REF
G1={USR1, ...}
G2={USR2, ...}
USR2 =
Rgt(Dlg, T=T1, T2, T3)
BDRQ
D, H, IDU, GUI
ADM
SYS
SES1
MSG
M1
PLGN1
UI1
PC1
RQ
PC2
UI2
MOD2
MODUI2
DDE
USR2

FIG. 3

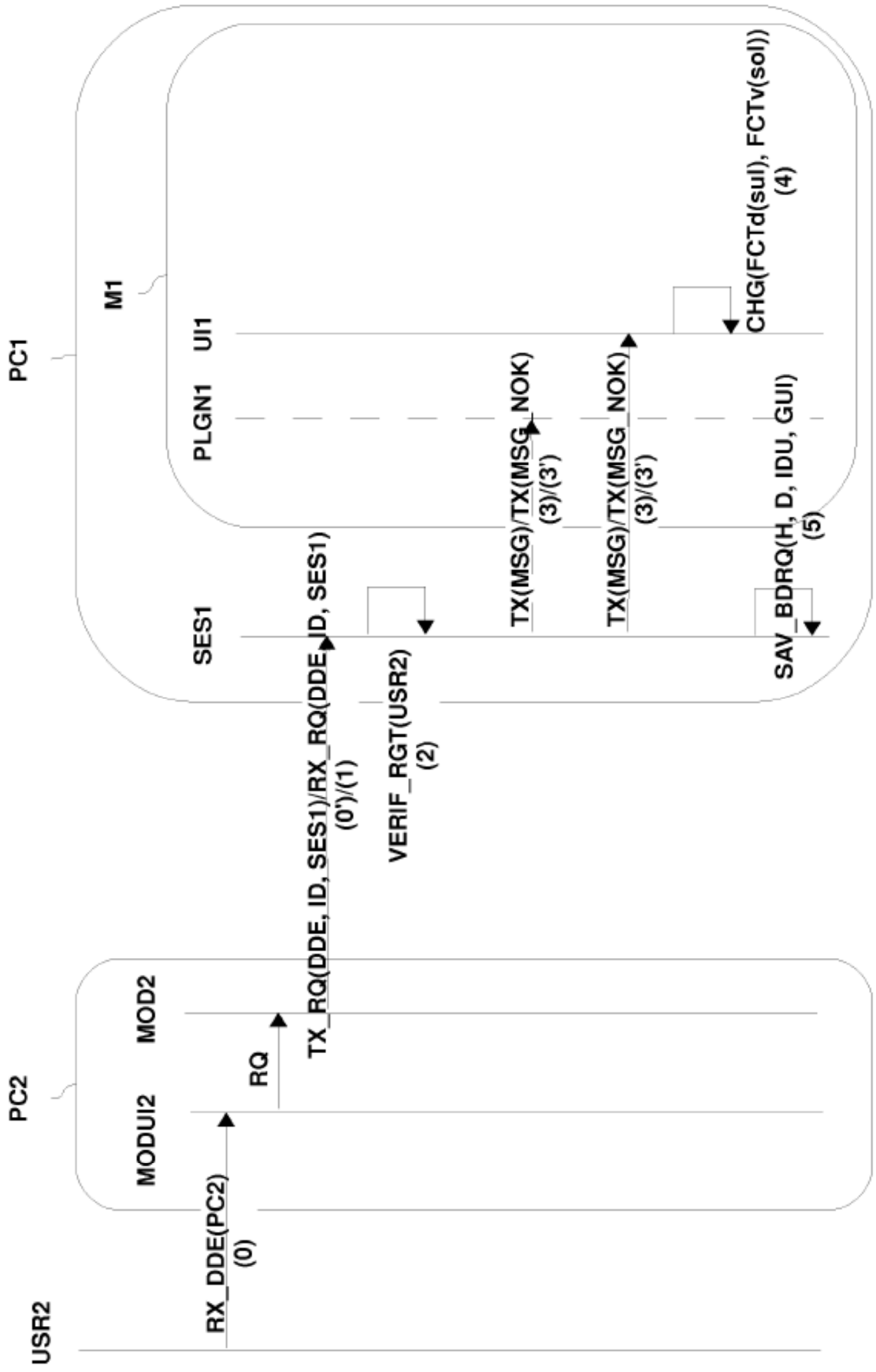
USR2
PC2
MODUI2
MOD2
PC1
M1
PLGN1
UI1
SES1
RX_DDE(PC2)
(0)
RQ
TX_RQ(DDE, ID, SES1)/RX_RQ(DDE, ID, SES1)
(0')/(1)
VERIF_RGT(USR2)
(2)
TX(MSG)/TX(MSG_NOK)
(3)/(3')
TX(MSG)/TX(MSG_NOK)
(3)/(3')
CHG(FCTd(sul), FCTv(sol))
(4)
SAV_BDRQ(H, D, IDU, GUI)
(5)

FIG. 4

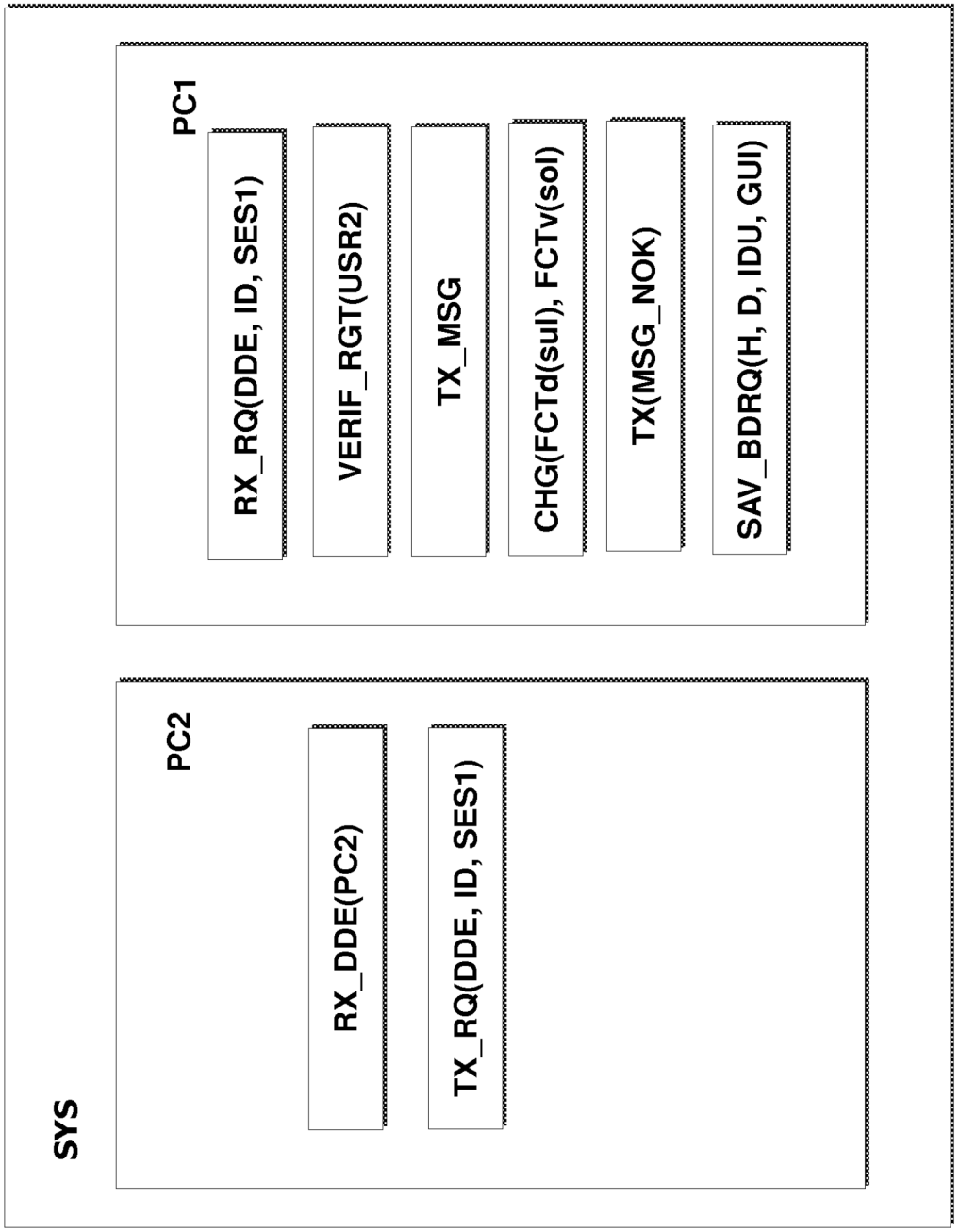
SYS
PC1
RX_RQ(DDE, ID, SES1)
VERIF_RGT(USR2)
TX_MSG
CHG(FCTd(sul), FCTv(sol)
TX(MSG_NOK)
SAV_BDRQ(H, D, IDU, GUI)
PC2
RX_DDE(PC2)
TX_RQ(DDE, ID, SES1)

FIG. 5

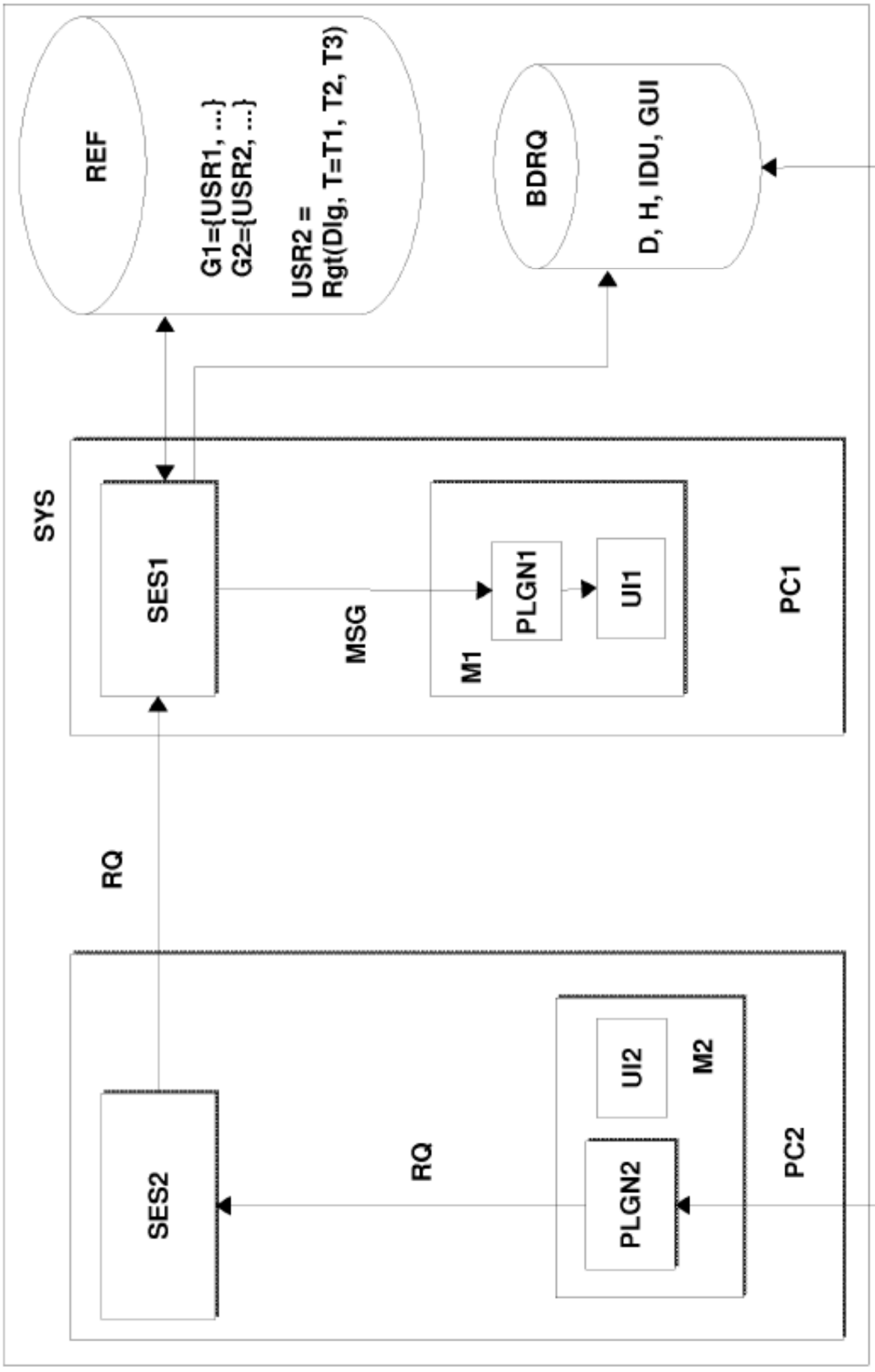
REF
G1={USR1, ...}
G2={USR2, ...}
USR2 =
Rgt(Dlg, T=T1, T2, T3)
BDRQ
D, H, IDU, GUI
ADM
SYS
SES1
MSG
M1
PLGN1
UI1
PC1
RQ
SES2
RQ
UI2
M2
PLGN2
PC2
DDE
USR2

FIG. 6