

REIVINDICACIONES

Habiéndose descrito la invención como antecede, se reclama como propiedad lo contenido en las siguientes reivindicaciones:

1. Procedimiento de gestión de la ejecución de una operación principal (OP1, OP2) por un elemento seguro (100), estando el procedimiento caracterizado porque: la operación principal está formada por una pluralidad de operaciones elementales (OP1_1, OP1_2, OP1-n), y el procedimiento comprende las siguientes etapas:
 - a. recibir (300, 400), de un equipo anfitrión, un comando (X, X1, X2, XN) en el formato de unidad de datos de protocolo de aplicación, APDU,
 - 15 b. activar (305) un contador de tiempo (130) durante la ejecución del comando de APDU con el fin de determinar una duración real de tratamiento del comando de APDU por el elemento seguro;
 - c. determinar (320) si la duración real de tratamiento (T_{ejecución}) indicada por el contador de tiempo es inferior a una duración predefinida (T_{máx}) asociada al comando de APDU;
 - d. en caso de determinación positiva, ejecutar (325) una o varias de dichas operaciones elementales durante el tiempo restante (T_{dispo}) de dicha duración predefinida; y
 - 25 e. enviar (330) una respuesta (Y, Y1, Y2, YN) al comando de APDU con destino al equipo anfitrión, tras la etapa d.
2. Procedimiento según la reivindicación 1, en el que la respuesta (Y, Y1, Y2, YN) al comando se envía al caducar la duración predefinida (T_{máx}) asociada al comando de APDU.
- 30 3. Procedimiento según una de las reivindicaciones anteriores, en el que el contador de tiempo (130) se activa tras la recepción (300, 400) del comando de APDU.

4. Procedimiento según una de las reivindicaciones anteriores, que comprende una pluralidad de iteraciones de las etapas a. a d. de manera que se ejecuta dicha pluralidad de operaciones elementales que forman la operación principal.
5. Procedimiento según una de las reivindicaciones anteriores, que comprende, tras el envío de una respuesta (Y, Y1, Y2, YN) a un comando de APDU recibido y previamente a la recepción de un siguiente comando de APDU (X, X1, X2, XN), la ejecución adicional (455) de una o varias de dichas operaciones elementales.
6. Procedimiento según la reivindicación anterior, en el que la ejecución adicional de una o varias de dichas operaciones elementales comprende la ejecución sucesiva de una o varias operaciones elementales hasta la recepción del siguiente comando de APDU.
7. Procedimiento según una de las reivindicaciones 1 a 6, en el que la operación principal (OP1, OP2) se divide previamente para dar dicha pluralidad de operaciones elementales (OP1_1, OP1_2, OP1_n), estando cada una asociada a una duración de tratamiento elemental (T_{estim}), y la etapa d. comprende la selección de la una o varias de dichas operaciones elementales que van a ejecutarse en función de sus duraciones de tratamiento elemental asociadas y de dicho tiempo restante (T_{dispo}).
8. Procedimiento según la reivindicación anterior, en el que la etapa d. comprende la ejecución de al menos dos operaciones elementales procedentes de al menos dos operaciones principales distintas.
9. Procedimiento según una de las reivindicaciones 1 a 6, en el que la etapa d. comprende la continuación de una ejecución de la operación principal desde un punto de

suspensión anterior, suspendiéndose dicha ejecución de la operación principal en un siguiente punto de suspensión que depende del tiempo restante.

10. Elemento seguro (100) configurado para ejecutar una
5 operación principal (OP1, OP2) formada por una pluralidad de operaciones elementales (OP1_1, OP1_2, OP1_n), comprendiendo el elemento seguro un procesador configurado para:
- a. recibir, de un equipo anfitrión, un comando (X, X1, X2, XN) en el formato de unidad de datos de protocolo de
10 aplicación, APDU,
 - b. activar un contador de tiempo (130) durante la ejecución del comando de APDU con el fin de determinar una duración real de tratamiento del comando de APDU por el elemento seguro;
 - 15 c. determinar si la duración real de tratamiento ($T_{\text{ejecución}}$) indicada por el contador de tiempo es inferior a una duración predefinida ($T_{\text{máx}}$) asociada al comando de APDU;
 - d. en caso de determinación positiva, ejecutar una o varias de dichas operaciones elementales durante el tiempo restante
20 (T_{dispo}) de dicha duración predefinida; y
 - e. enviar una respuesta (Y, Y1, Y2, YN) al comando de APDU con destino al equipo anfitrión, tras la etapa d.
11. Soporte no transitorio legible por ordenador que almacena un programa informático que, cuando se ejecuta por
25 un elemento seguro dotado de un procesador, hace que el elemento seguro realice el procedimiento según una de las reivindicaciones 1 a 9.