

REIVINDICACIONES

1. Un método para sellar datos de enclave, que comprende:
enviar (2002), a un enclave de origen (1912) alojado en una primera plataforma de enclave nativa (1916), un primer reporte de afirmación de un enclave de sellado (1932) alojado en una segunda plataforma de enclave nativa (1936);
recibir (2004) una lista permitida y datos de enclave asociados del enclave de origen en el enclave de origen, en donde la lista permitida es una lista de tipos de identidad abstracta que corresponden a respectivos niveles de jerarquía de una jerarquía de identidad e incluye una lista de una o más identidades de enclave permitidas para desellar los datos de enclave;
almacenar (2006) de manera segura los datos de enclave y la lista permitida, en donde el almacenado de manera segura incluye cifrar los datos de enclave con una clave asociada con el enclave de sellado, por parte del enclave de sellado, antes de recibir una petición por los datos de enclave de parte de un enclave de destino para crear datos de enclave sellados; y
restringir (2008, 2010, 2012) el acceso de los datos de enclave a enclaves con identidades autenticadas que se permite de acuerdo con la lista permitida, en donde la restricción incluye determinar si enviar los datos de enclave desde el enclave sellado al enclave de destino, el cual es diferente del enclave de sellado, con base al menos en parte en si el enclave de destino está incluido en la lista de una o más identidades de enclave permitidas para desellar los datos de enclave.
2. El método de acuerdo con la reivindicación 1, en donde:
la primera plataforma de enclave nativa está en una primera computadora y la segunda plataforma de enclave nativa está alojada en una segunda computadora.
3. El método de acuerdo con la reivindicación 1 que comprende además:
recibir un reporte de afirmación de origen del enclave de origen; y
derivar un valor de identidad permitida a partir del reporte de afirmación de origen y un tipo de identidad abstracta en la lista permitida.
4. El método de acuerdo con la reivindicación 1, en donde se cifran los datos de enclave recibidos, y que comprende además:
ejecutar un proceso de afirmación entre el enclave de origen y el enclave de sellado; y
descifrar los datos de enclave cifrados con una clave generada durante el proceso de afirmación.
5. El método de acuerdo con la reivindicación 1, en donde almacenar de manera segura los datos de enclave incluye:
almacenar los datos de enclave sellados en almacenamiento persistente; y
en donde restringir el acceso de los datos de enclave a enclaves con identidades autenticadas adicionalmente incluye:
después de determinar que los datos de enclave son enviados desde el enclave sellado al enclave de destino con base al menos en parte en que el enclave de destino está incluido en la lista de una o

más identidades de enclave permitidas para desellar los datos de enclave, descifrar los datos de enclave sellados en respuesta a recibir la petición por los datos de enclave de parte de un enclave de destino.

6. El método de acuerdo con la reivindicación 1, en donde una o más identidades de enclave en la lista permitida son especificadas por una o más claves públicas del respectivo uno o más enclaves.

7. Un método para sellar datos de enclave, que comprende:
recibir, en un enclave de origen (1912) alojado en una primera plataforma de enclave nativa (1916), un primer reporte de afirmación de un enclave de sellado (1932) alojado en una segunda plataforma de enclave nativa (1936);
verificar la confianza en el enclave de sellado; y
enviar una lista permitida y datos de enclave asociados hacia el enclave de sellado, en donde la lista permitida incluye una lista de una o más identidades de enclave permitidas para desellar los datos de enclave, dicho envío comprende causar que el enclave de sellado determine si enviar los datos de enclave hacia el enclave de destino que es diferente del enclave de sellado con base al menos en parte en si el enclave de destino está incluido en la lista de una o más identidades de enclave permitidas para desellar los datos de enclave, en donde la lista permitida es una lista de tipos de identidad abstracta que corresponden a respectivos niveles de jerarquía de una jerarquía de identidad; y.
enviar un reporte de afirmación de origen del enclave de origen hacia el enclave de sellado, en donde el reporte de afirmación de origen incluye al menos un valor de identidad del enclave de origen que corresponde a un tipo de identidad abstracta en la lista permitida.

8. El método de acuerdo con la reivindicación 7 que comprende además:
un proceso de afirmación entre el enclave de sellado y el enclave de origen;
generar datos de enclave cifrados por medio de cifrar los datos de enclave con una clave generada durante el proceso de afirmación; y
en donde los datos de enclave enviados hacia el enclave de sellado son los datos de enclave cifrados.

9. El método de acuerdo con la reivindicación 7, en donde:
la primera plataforma de enclave nativa está en una primera computadora y la segunda plataforma de enclave nativa está alojada en una segunda computadora.

10. El método de acuerdo con la reivindicación 7, que comprende además:
completar parcialmente una operación de procesamiento seguro en el enclave de origen; y
en donde los datos de enclave incluyen datos de estado del enclave de origen suficientes para permitir que otra instanciación de enclave continúe la operación de procesamiento seguro completada parcialmente.

11. Un sistema que comprende al menos un procesador y memoria que almacena, en la misma, instrucciones que, cuando son ejecutadas por el sistema, provocan al menos:

Enviar (2002), a un enclave de origen (1912) alojado en una primera plataforma de enclave nativa (1916), un primer reporte de afirmación de un enclave de sellado (1932) alojado en una segunda plataforma de enclave nativa (1936);

recibir (2004) una lista permitida y datos de enclave asociados del enclave de origen, en donde la lista permitida es una lista de tipos de identidad abstracta que corresponden a respectivos niveles de jerarquía de una jerarquía de identidad e incluye una lista de una o más identidades de enclave permitidas para desellar los datos de enclave;

almacenar (2006) de manera segura los datos de enclave y la lista permitida, en donde el almacenado incluye cifrar los datos de enclave con una clave asociada con el enclave de sellado, por parte del enclave de sellado, antes de recibir una petición por los datos de enclave de parte de un enclave de destino para crear datos de enclave sellados; y

restringir (2008, 2010, 2012) el acceso de los datos de enclave a enclaves con identidades autenticadas que se permite de acuerdo con la lista permitida, en donde la restricción incluye determinar si enviar los datos de enclave desde el enclave sellado al enclave de destino, el cual es diferente del enclave de sellado, con base al menos en parte en si el enclave de destino está incluido en la lista de una o más identidades de enclave permitidas para desellar los datos de enclave.

12. El sistema de acuerdo con la reivindicación 11, en donde:

la primera plataforma de enclave nativa está en una primera computadora y la segunda plataforma de enclave nativa está alojada en una segunda computadora.

13. El sistema de acuerdo con la reivindicación 11, en donde las instrucciones provocan además al menos:

recibir un reporte de afirmación de origen del enclave de origen; y
derivar un valor de identidad permitida a partir del reporte de afirmación de origen y un tipo de identidad abstracta en la lista permitida.

14. El sistema de acuerdo con la reivindicación 11, en donde se cifran los datos de enclave recibidos, y las instrucciones provocan además al menos:

ejecutar un proceso de afirmación entre el enclave de origen y el enclave de sellado; y
descifrar los datos de enclave cifrados con una clave generada durante el proceso de afirmación.

15. El sistema de acuerdo con la reivindicación 11, en donde almacenar de manera segura los datos de enclave además incluye:

almacenar los datos de enclave sellados en almacenamiento persistente; y
en donde restringir el acceso de los datos de enclave a enclaves con identidades autenticadas adicionalmente incluye:

después de determinar que los datos de enclave son enviados desde el enclave sellado al enclave de destino con base al menos en parte en que el enclave de destino está incluido en la lista de una o más identidades de enclave permitidas para desellar los datos de enclave, descifrar los datos de enclave sellados en respuesta a recibir la petición por los datos de enclave de parte de un enclave de destino.

16. El sistema de acuerdo con la reivindicación 11, en donde una o más identidades de enclave en la lista permitida son especificadas por una o más claves públicas de los respectivos uno o más enclaves.

17. Un sistema que comprende al menos un procesador y memoria que almacena en la misma instrucciones que, cuando son ejecutadas por el sistema, provocan al menos:

recibir, en un enclave de origen (1912) alojado en una primera plataforma de enclave nativa (1916), un primer reporte de afirmación de un enclave de sellado (1932) alojado en una segunda plataforma de enclave nativa (1936);

verificar la confianza en el enclave de sellado;

enviar una lista permitida y datos de enclave asociados hacia el enclave de sellado, en donde la lista permitida incluye una lista de una o más identidades de enclave permitidas para desellar los datos de enclave, dicho envío comprende causar que el enclave de sellado determine si enviar los datos de enclave hacia el enclave de destino que es diferente del enclave de sellado con base al menos en parte en si el enclave de destino está incluido en la lista de una o más identidades de enclave permitidas para desellar los datos de enclave, en donde la lista permitida es una lista de tipos de identidad abstracta que corresponden a respectivos niveles de jerarquía de una jerarquía de identidad; y.

enviar un reporte de afirmación de origen del enclave de origen hacia el enclave de sellado, en donde el reporte de afirmación de origen incluye al menos un valor de identidad del enclave de origen que corresponde a un tipo de identidad abstracta en la lista permitida.

18. El sistema de acuerdo con la reivindicación 17, en donde las instrucciones provocan además al menos:

un proceso de afirmación entre el enclave de sellado y el enclave de origen;

generar datos de enclave cifrados al cifrar los datos de enclave con una clave generada durante el proceso de afirmación; y

en donde los datos de enclave enviados al enclave de sellado son los datos de enclave cifrados.

19. El sistema de acuerdo con la reivindicación 17, en donde:

la primera plataforma de enclave nativa está en una primera computadora y la segunda plataforma de enclave nativa está alojada en una segunda computadora.

20. El sistema de acuerdo con la reivindicación 17, en donde las instrucciones provocan además al menos:

completar parcialmente una operación de procesamiento seguro en el enclave de origen; y

en donde los datos de enclave incluyen datos de estado del enclave de origen suficientes para permitir que otra instanciación de enclave continúe la operación de procesamiento seguro completada parcialmente.