

CAPÍTULO REIVINDICATORIO

1. Un sistema (100) para permitir una comunicación de al menos un grupo de credenciales controladas correspondientes a un presentador desde un servidor a un punto final de red, dicho sistema caracterizado porque comprende:

al menos un punto final de red;

al menos un aparato de aceptación (109) configurado para enviar una comunicación de aparato de aceptación (104), dicha comunicación de aparato de aceptación contiene un código clave secreto obtenido (109a) que pertenece a dicho presentador y un código clave compartido una vez apagado (109b), y dicho aparato de aceptación comprende un procesador del aparato de aceptación, una interfaz del aparato de aceptación, memoria del aparato de aceptación, y al menos una de una consola de entrada del aparato de aceptación y una consola de salida del aparato de aceptación;

al menos un aparato de presentación (108) configurado para enviar una comunicación de aparato de presentación (105), dicha comunicación de aparato de presentación contiene un identificador de presentador (108a) que pertenece a dicho presentador y dicho código clave compartido una vez apagado (108b) , y dicho aparato de presentación comprende un procesador del aparato de presentación, una interfaz del aparato de presentación, memoria del aparato de presentación, y al menos una de una consola de entrada de aparato de presentación y una consola de salida del aparato de presentación;

al menos un servidor que comprende un procesador de servidor, al menos una interfaz de comunicaciones de servidor y una memoria de servidor que almacena:

(i) al menos una entrada (103) que pertenece a dicho al menos un grupo de credenciales controladas correspondientes al presentador,

(ii) cada entrada está afiliada al menos a un registro (102), el registro que pertenece a cualquier presentador y comprende un identificador grabado de presentador y un código clave secreto grabado unido al identificador grabado de presentador;

en donde dicho al menos un servidor está configurado para:

a) recibir dicha comunicación de aparato de aceptación (104);

- 5 b) recibir dicha comunicación de aparato de presentación (105);
- c) buscar una coincidencia de dicho código clave compartido una vez
 apagado (109b) contenido en dicha comunicación de aparato de
 aceptación (104) con dicho código clave compartido una vez apagado
 (108b) contenido en dicha comunicación de aparato de presentación
 (105);
- 10 d) iniciar una búsqueda de un registro objetivo al conectar dicho código
 clave secreto obtenido en dicha comunicación de aparato de aceptación
 (104) con dicho identificador de presentador obtenido en dicha
 comunicación de aparato de presentación (105), ambas de dicha
 comunicación de aparato de aceptación y dicha comunicación de
 aparato de presentación contienen el mismo código clave compartido
 una vez apagado (108b, 109b);
- 15 e) conducir la búsqueda de dicho registro objetivo que comprende un
 código clave secreto grabado e identificador grabado de presentador
 que son iguales ambos de dicho código secreto (109a) y dicho
 identificador grabado de presentador (108a);
- f) Completar una búsqueda al identificar una entrada (103) afiliada con
 dicho registro objetivo;
- 20 g) permitir la recuperación de dicho al menos un grupo de credenciales
 controladas que pertenecen a dicha entrada (103) y permiten la
 liberación de dicho al menos un grupo de credenciales controladas a
 dicho punto final de red (110), dicho punto final de red es un receptor
 permitido de dicho al menos un grupo de credenciales controladas
- 25 correspondientes al presentador.

2. El sistema de conformidad con la Reivindicación 1, caracterizado porque dicho al
 menos un servidor comprende un servidor de control (101).
- 30 3. El sistema de conformidad con la Reivindicación 2, caracterizado porque el servidor
 de control (101) además está configurado para generar dicho código clave
 compartido una vez apagado, y hacerlo disponible en el aparato de aceptación
 (109).

- 5 4. El sistema de conformidad con la Reivindicación 2, caracterizado porque dicho aparato de aceptación además está configurado para generar dicho código clave compartido una vez apagado, recibir dicho código clave secreto obtenido (109a) de dicho presentador y transmitir dicha comunicación de aparato de aceptación a dicho servidor de control (101).
- 10 5. El sistema de conformidad con la Reivindicación 3, caracterizado porque dicho aparato de presentación además está configurado para recibir dicho código clave compartido una vez apagado de dicho aparato de aceptación (109), recuperar dicho identificador de presentador grabado de una memoria de dicho aparato de presentación y transmitir dicha comunicación de aparato de presentación (105) a dicho servidor de control (101).
- 15 6. El sistema de conformidad con cualquiera de las Reivindicaciones 1 a 5, caracterizado porque dicho registro comprende dicho identificador grabado de presentador y dicho código clave secreto grabado además comprende un alias asociado con el identificador de presentador y afiliado con dicha entrada (103) que pertenece a dicho al menos un grupo de credenciales controladas.
- 20 7. El sistema de conformidad con cualquiera de las Reivindicaciones 1 a 6, caracterizado porque dicha comunicación de aparato de presentación además contiene un alias asociado con dicho identificador de presentador obtenido y afiliado con dicha entrada (103) que pertenecen a dicho al menos un grupo de credenciales controladas, en donde dicha búsqueda de dicho registro objetivo
- 25 además utiliza dicho alias contenido en dicha comunicación de aparato de presentación (105) para buscar dicho registro objetivo que comprende dicho alias además de comprender dicho identificador obtenido de presentador (108a) y dicho código clave secreto obtenido.
- 30 8. El sistema de conformidad con cualquiera de las Reivindicaciones 1 a 7, caracterizado porque dicho punto final de red comprende dicho aparato de aceptación (109) y está configurado como un receptor designado de uno o más tipos de dicho al menos un grupo de credenciales controladas.

9. El sistema de conformidad con cualquiera de las Reivindicaciones 1 a 7, caracterizado porque dicho punto final de red está conectado a dicho aparato de aceptación y está configurado como un receptor designado de uno o más tipos de dicho al menos un grupo de credenciales controladas.

5

10. El sistema de conformidad con la Reivindicación 2, caracterizado porque dicho al menos un grupo de credenciales controladas comprende la entrada en dicho registro objetivo (102) en dicho servidor de control (101).

10

11. El sistema de conformidad con la Reivindicación 1, donde dicho al menos un servidor comprende un servidor de control (101) y un servidor diferente a dicho servidor de control, caracterizado porque el por lo menos un grupo de credenciales controladas comprende una entrada en el servidor diferente, donde la entrada en el servidor diferente está afiliada a dicho registro objetivo en dicho servidor de control (101).

15

12. El sistema de conformidad con cualquiera de las Reivindicaciones 1 a 11, caracterizado porque un periodo de validez es asignado a dicha comunicación de aparato de aceptación (104), y en donde el paso c) además comprende establecer si ha expirado dicho periodo de validez.

20

13. El sistema de conformidad con cualquiera de las Reivindicaciones 1 a 11, caracterizado porque se asigna un periodo de validez a dicha comunicación de aparato de presentación (105), y en donde el paso c) además comprende establecer si ha expirado dicho periodo de validez.

25

14. El sistema de conformidad con cualquiera de las Reivindicaciones 1 a 11, caracterizado porque se asigna un periodo de validez a dicho código clave compartido una vez apagado, y en donde el paso c) además comprende establecer si el periodo de validez ha expirado.

30

15. El sistema de conformidad con la Reivindicación 14, caracterizado porque dicho código clave compartido una vez apagado es único por la duración de dicho periodo de validez.

- 5 16. El sistema de conformidad con cualquiera de las Reivindicaciones 1 a 15, caracterizado porque dicha comunicación de aparato de aceptación (104) además contiene uno o más parámetros auxiliares predeterminados y dicha comunicación de aparato de presentación además también comprende dicho uno o más parámetros auxiliares predeterminados.
- 10 17. El sistema de conformidad con la Reivindicación 16, cuando depende de cualquiera de las Reivindicaciones 2 a 5, caracterizado porque dicho servidor de control (101) busca coincidir con al menos uno de dichos parámetros auxiliares predeterminados de dicha comunicación aparato de presentación (105) con dicho(s) parámetro(s) auxiliar predeterminado(s) correspondiente(s) de dicha comunicación - de aparato de aceptación (104) para proporcionar además al menos uno de: correlación y corroboración.
- 15 18. El sistema de conformidad con cualquiera de las Reivindicaciones 2 a 5, caracterizado porque, si dichos registros comprenden entradas de al menos un grupo de credenciales controladas en dicho servidor de control (101), se realizan los pasos f) y g) en dicho servidor de control, y la comunicación de dicho al menos un grupo de credenciales controladas se realiza a partir de dicho servidor de control.
- 20 19. El sistema de conformidad con cualquiera de las Reivindicaciones 2 a 5, caracterizado porque, si dichos registros comprenden entradas de al menos un grupo de credenciales controladas en un servidor diferente a dicho servidor de control, los pasos f) y g) se realizan en dicho servidor diferente, y la comunicación de dicho al menos un grupo de credenciales controladas se realiza utilizando uno de: dicho servidor de control y dicho servidor diferente.
- 25 20. El sistema de conformidad con cualquiera de las Reivindicaciones 2 a 5, caracterizado porque, si no se encuentra ninguna coincidencia entre dicha comunicación de aparato de aceptación (104) y comunicación de aparato de presentación (105) en dicho servidor de control (101), dicho servidor de control termina acciones adicionales configuradas y registra un estado de los eventos ahí.
- 30

- 5 21. El sistema de conformidad con cualquiera de las Reivindicaciones 2 a 5, caracterizado porque, sino se encuentra ningún registro objetivo en dicho servidor de control (101), dicho servidor de control termina acciones adicionales configuradas y registra un estado de los eventos ahí.
- 10 22. El sistema de conformidad con cualquiera de las Reivindicaciones 2 a 5, caracterizado porque dicho servidor de control (101) además está configurado para registrar un estado de los eventos que ocurren y para transmitir dicho estado al menos a uno de: dicho aparato de aceptación (109) y dicho aparato de presentación (108).
- 15 23. El sistema de conformidad con cualquiera de las Reivindicaciones 1 a 22, caracterizado porque cada uno de puntos finales de red (110), comprende un procesador de punto final de red, interfaz de comunicación de punto final de red, memoria de punto final de red, y al menos una de una consola de entrada de punto final de red y consola de salida de punto final de red.
- 20 24. El sistema de conformidad con cualquiera de las Reivindicaciones 1 a 23, caracterizado porque el sistema es operable por una red de comunicaciones (106, 107, 111).
- 25 25. Un método para permitir una comunicación de al menos un grupo de credenciales controladas correspondientes a un presentador de al menos un servidor a un punto final de red (110), dicho método comprende los siguientes pasos realizados por al menos un servidor:
- 30 a) Recibir, de un aparato de aceptación una comunicación de aparato de aceptación (104), dicha comunicación contiene un código clave secreto obtenido (109a) que pertenece a dicho presentador y un código clave compartido una vez apagado (109b) y dicho aparato de aceptación comprende un procesador del aparato de aceptación, una interfaz del aparato de aceptación, memoria del aparato de aceptación, y al menos una de una consola de entrada del aparato de aceptación y una consola de salida del aparato de aceptación;

- 5 b) Recibir, de un aparato de presentación una comunicación de aparato de presentación (105), dicha comunicación contiene un identificador obtenido de presentador (108a) que pertenece a dicho presentador y código clave compartido una vez apagado (108b) y dicho aparato de presentación comprende un procesador del aparato de presentación, una interfaz del aparato de presentación, memoria del aparato de presentación, y al menos una de una consola de entrada de aparato de presentación y una consola de salida del aparato de presentación;
- 10 c) Buscar, por el al menos un procesador de servidor de el al menos un servidor, una coincidencia de dicho código clave compartido una vez apagado (109b) contenido en dicha comunicación de aparato de aceptación (104) y dicho código clave compartido una vez apagado (108b) contenido en dicho comunicado de aparato de presentación (105);
- 15 d) Iniciar, por el al menos un procesador de servidor, una búsqueda de un registro objetivo al conectar dicho código clave secreto obtenido (109a) de dicha comunicación de aparato de aceptación (104) y dicho identificador obtenido de presentador (108a) en dicha comunicación de aparato de presentación (105), ambas de dicha comunicación de aparato de aceptación y dicha comunicación de aparato de presentación contienen el mismo código clave compartido una vez apagado (108b, 109b);
- 20 e) Conducir, por el al menos un procesador de servidor, la búsqueda del registro objetivo que comprende un código clave secreto grabado e identificador grabado de presentador que son iguales a tanto dicho código clave secreto obtenido (109a) y dicho identificador obtenido de presentador (108a);
- 25 f) Identificar, por el al menos un procesador de servidor, una entrada (103) afiliada con dicho registro de control, dicha entrada que pertenece a dicho al menos un grupo de credenciales controladas correspondientes a el presentador; y
- 30 g) Permitir, por el al menos un procesador de servidor, una recuperación de dicho al menos un grupo de credenciales controladas que pertenecen a dicha entrada y que permiten una liberación de dicho grupo de credenciales controladas a dicho punto final de red (110), dicho punto final es un receptor permitido de dicho al menos un grupo de credenciales controladas correspondientes a el presentador.

- 5 26. El método de conformidad con la Reivindicación 25 caracterizado porque el registro objetivo además comprende un alias asociado con dicho identificador obtenido de presentador (108a) y afiliado con dicha entrada (103) que pertenece a dicho al menos un grupo de credenciales controladas, y dicha comunicación de aparato de presentación (105) además contiene un alias asociado con dicho identificador obtenido de presentador (108a) y afiliado con dicha entrada que pertenece a dicho al menos un grupo de credenciales controladas, y en donde el paso (e) además comprende hacer coincidir alias respectivos de dicho registro y
10 dicha comunicación de aparato de presentación.
- 15 27. El método de conformidad con la Reivindicación 25 ó 26, caracterizado porque dicho al menos un servidor comprende un servidor de control (101) y los pasos (a) a (g) se realizan ahí.
- 20 28. El método de conformidad con la Reivindicación 25 ó 26, caracterizado porque al menos un servidor comprende un servidor de control (101) y un servidor diferente a dicho servidor de control, y donde dicho al menos un grupo de credenciales controladas comprende una entrada en dicho servidor diferente a dicho servidor de control (101), dicha entrada está afiliada con dicho registro objetivo, y en donde el paso de identificar un grupo de credenciales se realiza en dicho servidor diferente, y en donde los pasos (e) a (g) se realizan en uno de: dicho servidor de control (101) y dicho servidor diferente.
- 25 29. El método de conformidad con cualquiera de las Reivindicaciones 25 a 28, caracterizado porque además comprende asignar un periodo de validez al menos a uno de: dicha comunicación aparato de aceptación (104), dicha comunicación de aparato de presentación (105) y dicho código clave compartido una vez apagado, y (c) además comprende establecer si ha expirado dicho periodo de validez.
- 30 30. El método de conformidad con la Reivindicación 29, caracterizado porque dicho código clave compartido una vez apagado es único por la duración de dicho periodo de validez.

- 5 31. El método de conformidad con cualquiera de las Reivindicaciones 25 a 29, caracterizado porque cada una de dicha comunicación de aparato de presentación (105) y dicha comunicación de aparato de aceptación (104) además contiene uno o más parámetros auxiliares predeterminados, y en donde el paso (c) además comprende buscar una coincidencia de al menos uno de dichos parámetros auxiliares predeterminados en dicha comunicación de aparato de presentación con al menos uno de parámetros auxiliares predeterminados correspondientes en dicha comunicación de aparato de aceptación.
- 10 32. El método de conformidad con la Reivindicación 27, caracterizado porque dichos registros comprenden entradas de al menos un grupo de credenciales controladas en dicho servidor de control (101), que realiza los pasos (f) y (g) en dicho servidor de control, y el método además comprende liberar dicho al menos un grupo de credenciales controladas de dicho servidor de control.
- 15 33. El método de conformidad con la Reivindicación 25 o 26, caracterizado porque dicho al menos un servidor comprende un servidor de control (101), y, si dichos registros comprenden entradas de al menos un grupo de credenciales controladas en un servidor diferente a dicho servidor de control (101), realizar los pasos (f) y (g) en dicho servidor diferente, y el método además comprende liberar dicho al menos un grupo de credenciales controladas de uno de: dicho servidor de control y dicho servidor diferente.
- 20 34. El método de conformidad con la Reivindicación 27 o 28, caracterizado porque, si no se encuentra ninguna coincidencia entre dicha comunicación de aparato de aceptación (104) y comunicación de aparato de presentación (105), termina acciones adicionales configuradas y registra un estado de los eventos en dicho servidor de control (101).
- 25 35. El método de conformidad con la Reivindicación 27 ó 28, caracterizado porque, si no se encuentra ningún registro objetivo, termina acciones adicionales configuradas y registra un estado de los eventos ahí o en dicho servidor de control (101).
- 30

36. El método de conformidad con la Reivindicación 27 o 28, caracterizado porque además comprende registrar un estado de los eventos en dicho servidor de control (101) y confiar el estado a al menos a uno de: dicho aparato de aceptación (109) y dicho aparato de presentación (108).

Señor Director

NUEVAS CREACIONES

Superintendencia de Industria y Comercio

E. S. D.

Referencia: Expediente No. NC2016/0000575
Asunto: Solicitud de patente para: SISTEMA Y MÉTODO PARA COMUNICAR CREDENCIALES
Solicitante: PRIVITI PTE. LTD
Fecha de Solicitud: 03 de agosto de 2016

RESPUESTA A PRIMER EXAMEN DE PATENTABILIDAD

ANDRÉS RINCÓN USCÁTEGUI, identificado como aparece al pie de mi firma, en mi condición de apoderado de la sociedad solicitante de la patente de la referencia, doy respuesta al Oficio 3641, notificado por fijación en lista el 03 de abril de 2018, para lo cual solicité plazo el 21 de junio de 2018.

I. MODIFICACIONES AL CAPÍTULO REIVINDICATORIO

En respuesta al examen de patentabilidad, el solicitante decide aportar un Capítulo Reivindicatorio Modificado conformado por 36 Reivindicaciones en las que se han incluido las siguientes modificaciones:

1. Características técnicas esenciales de la Reivindicación 23 han sido incluidas en las Reivindicaciones 1 y 25.
2. La Reivindicación 23 fue modificada de tal manera que se eliminó la referencia a la materia que fue incluida en las Reivindicaciones 1 y 25 y ahora solo conserva la materia relacionada con los puntos finales de red.

INNOVACIÓN PARA LOS NEGOCIOS

BOGOTÁ DC, 110221 - COLOMBIA Edificio Siski - Carrera 4 No. 72-35 Teléfono (57-1) 347 3611 Fax (57-1) 211 8650
MEDELLÍN, 050021 - COLOMBIA San Fernando Plaza - Carrera 42 A No. 1-25 Torre 4 Oficina 303 Teléfono (57-4) 5204760
BARRANQUILLA, 080002- COLOMBIA - Calle 64 No. 50-22 Oficina 201 Teléfono (57-5) 351 6440

www.cavelier.com
cavelier@cavelier.com

3. Se agregó la aclaración entre los códigos clave secretos e identificadores de presentador que están grabados y los que son obtenidos en una comunicación en las Reivindicaciones 1, 4, 5, 6, 7, 8, 25 y 26. Esto con el fin de aportar claridad a la materia descrita.

4. Se modifico la mención al grupo de credenciales controladas en las Reivindicaciones 1, 6 a 11, 18, 19, 25, 26, 28, 32 y 33 para eliminar la mención a que están conectadas para mejorar la claridad del término.

5. Se modificaron las Reivindicaciones 11 y 28 para agregar la mención al servidor de control y un servidor diferente de a dicho servidor de control lo cual tiene soporte en el Capítulo Descriptivo en al menos la Página 18, Líneas 4 a 17.

6. Se modificaron las Reivindicaciones 20, 21, 22, 34 y 35 para aclarar que se terminan acciones adicionales configuradas y se registra un estado de los eventos. Esto con el fin de mejorar la claridad de la materia reclamada.

7. Se modificaron las dependencias de las Reivindicaciones 6, 7, 8, 11, 12, 16, 23, 24.

Estas modificaciones se ajustan al Artículo 34 de la Decisión 486 de 2000, ya que no constituyen una ampliación de la protección que correspondería a la divulgación contenida en la solicitud inicial.

II. EN CUANTO A LA CLARIDAD

En relación a los términos generales, me permito respetuosamente señalar que los términos objetados por el Examinador son perfectamente claros para toda persona del oficio normalmente versada en la materia y, más aún, todos están claramente descritos en el Capítulo Descriptivo de la Solicitud y presentan su respectiva referencia a las Figuras.

Las Reivindicaciones 1 a 36 fueron objetadas por supuestamente carecer de claridad y concisión por presentar los siguientes términos:

- i. "*Credenciales controladas*" (Reivindicaciones 1, 6 a 10, 18, 19, 25, 26, 28, 32 y 33)

- ii. "*punto final de red*" (Reivindicaciones 1, 8, 9, 23 y 25)
- iii. "*Aparato de aceptación*" (Reivindicaciones 1, 3 a 5, 9, 12, 16, 17, 20, 22, 25, 29, 31, 34 y 36)
- iv. "*Presentador*" (reivindicaciones 1, 4 a 7, 25 y 26)
- v. "*Código clave*" (Reivindicaciones 1, 3 a 7, 14, 15, 25, 26, 29 y 30)
- vi. "*Aparato de presentación*" (Reivindicaciones 1, 5, 7, 13, 16, 17, 20, 22, 25, 26, 29, 31, 34 y 36)
- vii. "*Identificador de presentador*" (Reivindicaciones 1, 6, 7, 25 y 26)
- viii. "*Registro objetivo*" (Reivindicaciones 1, 7, 10, 11, 21, 25, 28 y 35)
- ix. "*Servidor de control*" (Reivindicaciones 2 a 5, 10, 11, 18 a 22, 27, 28, 32, 33, 35 y 36)
- x. "*Alias*" (Reivindicaciones 6, 7 y 26)
- xi. "*Parámetros auxiliares*" (Reivindicaciones 16, 17 y 31)
- xii. "*Red de comunicaciones*" (Reivindicación 24).

En respuesta, el solicitante desea señalar que los términos objetados están claramente definidos y constantemente referenciados en el Capítulo Descriptivo de la presente solicitud. Adicionalmente, estos términos son entendidos y apreciados por una persona experta en la materia (PHOSITA) en el campo de las tecnologías de comunicación de la información y fueron seleccionados en todas las realizaciones para causar un efecto de permitir lecturas de información confidencial por parte de la(s) máquina(s) de destino de la(s) máquina(s) fuente(s). Por ejemplo, el Solicitante se refiere a las siguientes referencias y explicaciones de cada término objetado tal como aparece en la especificación:

Referencias al "*punto final de red*" (Reivindicaciones 1, 8, 9, 23 y 25):

Un punto final de red se diseña como lector de destino (máquina de lectura de documentos) de documentos de credenciales (documentos legibles por máquina), buscando ser designado destinatario de información confidencial:

- i. Es una máquina de punto final en la red de comunicaciones;
- ii. Es una máquina que comprende memoria, procesador, interfaces de comunicación;
- iii. Es una máquina que también puede comprender consolas de entrada de usuario y/o consolas de salida;

Un punto final de red es un dispositivo aceptante o está asociado a un dispositivo aceptante;

Es el punto de interacción para presentar y aceptar cualquier documento de credencial; requiere una lectura de información confidencial de los documentos de credenciales. Busca ser permitido o designado para solicitar y recibir una lectura de información confidencial de los documentos de credenciales.

Ver para. [0001], [0008], [0009], [0050], [0061], [0065] a [0067] y [0083]; Figura 10 del Capítulo Descriptivo de la solicitud.

Referencias a "*credenciales controladas*" (Reivindicaciones 1, 6 a 10, 18, 19, 25, 26, 28, 32 y 33):

Un instrumento emitido con credenciales controladas se describe como cualquier documento legible por máquina que contenga información confidencial, configurado para ser leído por cualquier punto final de red (máquina de lectura de documentos) que se le haya permitido ser el destinatario designado de la información confidencial sic.

Un conjunto de información confidencial se controla continuamente. Por un lado, y en el curso de la emisión, un conjunto de credenciales se controla en el documento legible por máquina. Por otro lado, y en el curso de la aceptación, la recuperación de credenciales está controlada por el presente que opera el dispositivo de presentación para indicar el documento de credencial (documento legible por máquina), y el presentador que opera el dispositivo acepta el lanzamiento de las credenciales para designar el punto final de red (máquina de lectura de documentos). Este es el caso desde la creación hasta el vencimiento de la información confidencial.

Ver párrafos [0001], [0002] a [0007] del Capítulo Descriptivo de la solicitud.

De manera similar, todos los términos objetados por el Examinador están soportados por las Figuras y el Capítulo Descriptivo. Quiero respetuosamente aclarar que, aunque se podría agregar la materia descrita en el Capítulo Descriptivo para cada uno de los términos objetados en las Reivindicaciones, la concisión y claridad del Capítulo Reivindicatorio resultaría afectada negativamente.

Adicionalmente, quisiera aclarar que el Solicitante está en derecho de reclamar la totalidad del concepto inventivo desarrollado, y especificar características no esenciales sólo limitaría el alcance de la patente. Así pues, considero superada la objeción.

Con base en todo lo anterior, considero que el Capítulo Reivindicatorio modificado adjunto cumple con todos los requisitos de claridad y concisión, ajustándose así a los lineamientos del Artículo 30 de la Decisión 486, ya que cualquier persona medianamente versada en la materia está en completa capacidad de reproducir la invención sin ambigüedad alguna.

III. ESTADO DE LA TÉCNICA

El Examinador determinó dos documentos como relevantes para realizar el análisis de patentabilidad de la presente patente de invención:

No.	Documento	Título	Fecha de Publicación
D1	US20130246203	<i>"Payment processing methods and systems"</i>	19 de septiembre de 2013
D2	WO2013034192	<i>"Method for validating an electronic transaction, and system thereof"</i>	14 de marzo de 2013

IV. EN CUANTO AL NIVEL INVENTIVO

Primero, hago un respetuoso llamado a la atención del Examinador acerca del Capítulo Reivindicatorio modificado adjunto en donde características técnicas esenciales de la antigua Reivindicación 23 fueron incluidas en las Reivindicaciones independientes 1 y 25 y se realizaron diferentes aclaraciones relacionadas con la diferencia entre los códigos clave secretos e identificadores de presentador que están grabados y los que son obtenidos y modificaciones de claridad que ayudan a comprender mejor la invención.

En relación con el nivel inventivo, respetuosamente difiero de la opinión del Examinador. Con el fin de demostrar el nivel inventivo de la presente invención, y basándome en la Guía para Examen de Solicitudes de Patente de Invención y Modelo de Utilidad (Guía de la SIC) sobre el método problema-solución, a continuación expongo cómo el arte previo citado por el Examinador no llevaría a la persona del oficio normalmente versada en la materia a la invención reclamada.

Identificar el estado de la técnica cercano a la invención reivindicada

El documento D1 puede ser considerado como el estado de la técnica cercano a la invención definida en las Reivindicaciones 1 y 25 porque divulga la implementación de un sistema para realizar transacciones de pago. De acuerdo con algunas realizaciones, las transacciones de pago pueden realizarse entre un consumidor que opera un dispositivo móvil y un comerciante (Pág. 1, Párr. 0003).

Determinar la diferencia entre la invención y estado de la técnica cercano

El solicitante no está de acuerdo en que la única diferencia encontrada entre el sistema descrito en la Reivindicación 1 y D1 consiste en que el sistema descrito en la Reivindicación 1 simplemente incluye *"una etapa de búsqueda de un código secreto que es conocido entre dos partes para completar la transacción"*; y el Solicitante tampoco está de acuerdo en que el efecto logrado al incluir simplemente cualquier búsqueda de cualquier código secreto sea *"garantizar la confiabilidad y seguridad de los datos intercambiados durante la transacción"*.

D1 se refiere al procesamiento de transacciones. D1 comienza con los detalles de la cuenta del pagador almacenados en el Servidor del sistema de manejo de transacciones (TMS) y finaliza con la transacción procesada en el Servidor del TMS. Por un lado, excluye cualquier verificación del procesamiento de transacciones en el Servidor del TMS con PIN; Por otro lado, impide cualquier transmisión de información de cuenta de pagador por parte de cualquier Dispositivo o Servidor a cualquier punto de venta (POS) de comerciante.

D1 involucra a los clientes que usan dispositivos móviles para realizar transacciones de pago en el servidor para liquidar compras en establecimientos comerciales y *"en los cuales los comerciantes no almacenan, capturan o transmiten la información de la tarjeta de pago"* (Página 1, Párrafo [0003]). D1 aborda la amenaza del robo de información de la cuenta de pago a través de los sistemas comerciales. Para ello, D1 introduce un sistema de gestión de transacciones (un servidor y un móvil) con acceso a información de cuentas de pago almacenadas, y evita la captura de información de cuentas de pago de tarjetas de

pago o dispositivos móviles o máquinas servidor en una terminal POS de un sistema comercial durante una transacción realizada en las máquinas servidor.

La presente invención, por otro lado, se refiere a presentadores que ofrecen grupos de credenciales durante intercambios con otros individuos u organizaciones (Párrafo [0007]). La presente invención es aplicable más allá de los pagos a la banca, finanzas, aviación, viajes, seguridad nacional, control de fronteras, energía, transporte, venta minorista y/o telecomunicaciones (Párrafo [0048]). La presente invención, a diferencia de D1, implica presentadores que usan pares de dispositivos de control para coordinar la comunicación de conjuntos de credenciales desde los servidores hasta los puntos finales de red cuando interactúan en los puntos finales de red. Si se aplica a pagos, la presente invención aborda la amenaza de mal manejo y uso indebido de una tarjeta de pago que contiene información de cuenta de pago (como grupo de credenciales) en un terminal POS (como punto final de red). Para hacer esto, la presente invención introduce un servidor de control que recibe comunicaciones de dispositivos de aceptación (integrados con puntos finales de red) y de dispositivos de presentación (asociados con grupos de credenciales en servidores) que busca permitir la captura de una lectura de un grupo de credenciales en un punto final de red desde un servidor durante una interacción solo si lo permite el titular legítimo del conjunto de credenciales.

D1 no enseña varias características de la presente invención, que incluyen, pero no se limitan a, al menos, las siguientes características que implican un servidor de control con un par de dispositivos de control de la Reivindicación 1:

- i. servidor que almacena ... (a) una entrada perteneciente a credenciales controladas ... dicha entrada afiliada con ... (b) un registro que comprende ... un código clave secreto vinculado al identificador de presentador;
- ii. servidor recibiendo ... un par de mensajes de control de un par de dispositivos de control ... que implica (a) comunicación del dispositivo de aceptación ... que contiene un código clave compartido una vez apagado y un código clave secreto relacionado al Presentador, ... y (b) comunicación del dispositivo de presentación ... que contiene un código clave compartido una vez apagado y un identificador de presentador relacionado al Presentador;

- iii. búsqueda de servidor ... para registro que contiene (a) un código clave secreto que es el mismo que el código clave secreto contenido en la comunicación del dispositivo receptor, vinculado a (b) un identificador de presentador que es el mismo que el identificador de presentador contenido en la presentación comunicación de dispositivo, en la que ambas comunicaciones contienen el mismo código clave compartido una vez apagado;

Si la búsqueda es exitosa y una entrada es identificable, el efecto causado es permitir la comunicación de credenciales controladas por el Servidor al Punto final de la red (asociado al dispositivo de aceptación).

Si la búsqueda no es exitosa y una entrada no es identificable, el efecto causado es la denegación de la comunicación de las credenciales controladas por el Servidor al Punto final de la red (asociado al dispositivo de aceptación).

El efecto logrado por estas diferencias es determinar si la lectura del documento en el servidor que se va a capturar en el punto final de red **está o no permitido** por el titular legítimo (el presentador) de un documento legible por máquina (que contiene un grupo de credenciales controladas).

Definir el efecto técnico causado y atribuible al elemento diferencial y deducir el problema técnico objetivo

El solicitante no está de acuerdo con el Examinador en que el problema técnico objetivo que la presente invención pretende resolver, formulado sobre la base de D1, es *"¿cómo modificar el método conocido en D1 para garantizar la confiabilidad y seguridad de los datos intercambiados durante la transacción?"*.

En cambio, el problema técnico objetivo correcto que la presente invención intenta resolver es *"cómo modificar el sistema de D1 para controlar la captura de una lectura de un documento legible por máquina en un punto final de red durante una interacción con el fin de garantizar el permiso del titular legítimo del documento para que una lectura sea capturada en el punto final de la red"*.

Evaluar si la invención reivindicada, partiendo del estado de la técnica cercano y del problema técnico objetivo, habría sido obvia para la persona medianamente versada en la materia

D2 se refiere a la verificación de transacciones electrónicas ([0002]) la cual comienza con la transmisión de información de identificación (como credenciales controladas) a un POS (como punto final de red) como se describe en el paso 100 "*iniciar una transacción electrónica que transmite información de identificación inalámbrica desde un módulo de pago electrónico (11) de un teléfono móvil (10) a un Terminal de POS (20), que envía dicha información de identificación junto con datos de transacción a una red minorista (21) y a un servidor (30), ...*". Después de la transmisión de la información de identificación, se proporciona un PIN de validación por separado "*vocalmente*" o "*textualmente*" a dicho servidor que tiene un efecto de control en el procesamiento de la transacción en dicho servidor. El uso de cualquier PIN no controló la transmisión de la información de identificación (como credenciales controladas) al POS (como punto final de red). D2 finaliza verificando la transacción en el servidor, no transmitiendo información de identificación en el servidor al terminal POS (como punto final de red).

Además, en D2, se captura un PIN de validación en el dispositivo móvil (PCD del cliente) (no en el POS del comerciante) y se proporciona al servidor (TMS de pago, no al POS del comerciante). Por lo tanto, obtener un código clave secreto en un aparato de aceptación asociado a cualquier punto final de red (POS del comerciante) y transmitir una comunicación del aparato de aceptación que contiene un código clave compartido y un código clave secreto al servidor (TMS de pago) no se enseña ni menciona en D2, ya que D2 no ha divulgado capturar ningún PIN de validación en el punto de venta del comerciante y transmitirlo al TMS de pago, a fin de permitir la comunicación de credenciales entre el servidor y el punto final de red (POS del comerciante).

Además, en D2, recuperar un identificador de presentador en cualquier aparato de presentación (PCD del cliente) y transmitir cualquier comunicación del dispositivo de presentación un código clave compartido y un identificador de presentador al servidor (TMS de pago) no se enseña ni se revela en D2, ya que D2 no divulga la recuperación de ningún identificador de presentador en el PCD del Cliente y la transmisión al TMS de pago.

D2 solo divulga el ingreso de un PIN en la PCD del cliente y la entrega al TMS de pago. Por lo tanto, una persona experta en la técnica no sería capaz de concebir la recuperación de ningún identificador de presentador en cualquier PCD de cliente y proporcionar cualquier identificador de presentador al TMS de pago sin llevar a cabo la actividad inventiva.

Por el contrario, la presente invención comienza con credenciales controladas en el Servidor, cuya lectura es requerida por el Punto final de Red; un código clave secreto en la Reivindicación 1 tiene un efecto de control al permitir la transmisión de credenciales controladas por el servidor al punto final de red. El uso del código clave secreto no controla el procesamiento de transacciones en el servidor como en D2. La presente invención finaliza permitiendo o no permitiendo la transmisión de credenciales controladas en el servidor al punto final de red, sin ningún procesamiento de transacción en el servidor o el punto final de red.

Si un experto en la técnica combinara D1 y D2, resultaría en que los clientes:

- (i) accederían a la información de la cuenta de pago en el Servidor del TMS utilizando su Dispositivo de computación móvil (PCD del cliente) para evitar el manejo de cualquier información de cuenta de pago en el POS del comerciante (enseñanzas de D1); y
- (ii) proporcionarían un PIN de validación al servidor (TMS de pago) desde su dispositivo móvil (PCD del cliente) para evitar la captura y el procesamiento de cualquier PIN de validación en el POS del comerciante (enseñanzas de D2).

Mientras que la combinación de D1 con D2 puede "*garantizar la confiabilidad y seguridad de los datos intercambiados durante la transacción*" en el Servidor del TMS, cualquier combinación y/o modificación de D1 con D2 nunca enseñaría al menos las siguientes características que involucran un servidor de control con un par de dispositivos de control de la Reivindicación 1 para permitir la comunicación de las credenciales controladas en el Servidor (TMS de pago) al Punto final de red (POS del comerciante):

- i. servidor que almacena ... (a) una entrada perteneciente a credenciales controladas ... dicha entrada afiliada con ... (b) un registro que comprende ... un código clave secreto vinculado al identificador de presentador;

- ii. servidor recibiendo ... un par de mensajes de control de un par de dispositivos de control ... que implica (a) comunicación del dispositivo de aceptación ... que contiene un código clave compartido una vez apagado y un código clave secreto relacionado al Presentador, ... y (b) comunicación del dispositivo de presentación ... que contiene un código clave compartido una vez apagado y un identificador de presentador relacionado al Presentador;
- iii. búsqueda de servidor ... para registro que contiene (a) un código clave secreto que es el mismo que el código clave secreto contenido en la comunicación del dispositivo receptor, vinculado a (b) un identificador de presentador que es el mismo que el identificador de presentador contenido en la presentación comunicación de dispositivo, en la que ambas comunicaciones contienen el mismo código clave compartido una vez apagado;

Además, en ausencia de identificar una entrada afiliada a un registro que comprenda (a) un código clave secreto que sea el mismo que el código clave secreto contenido en la comunicación del aparato de aceptación, y (b) un identificador de presentador que sea el mismo que el identificador de presentador contenido en la comunicación del aparato de presentación (donde ambos mensajes contienen el mismo código clave compartido una vez apagado), permitiendo la comunicación de credenciales controladas por el servidor al punto final de red (asociado al aparato de aceptación) no es un efecto causado por cualquier combinación modificada de D1 y D2.

De manera complementaria, presento un resumen de las aclaraciones del solicitante en la Tabla 1 del presente memorial que concentra las principales diferencias entre el estado de la técnica y la presente solicitud.

Tabla 1. Resumen de las aclaraciones del solicitante.

Opinión del Examinador	Aclaración del Solicitante
El documento D1 se considera el estado de la técnica más cercano a la invención definida en la Reivindicación 1 porque divulga la implementación de un método para realizar transacciones de pago. De acuerdo con algunas realizaciones, las transacciones de pago pueden realizarse entre un consumidor que opera un dispositivo móvil y un comerciante (Pág. 1, Párr. 0003)	D1 aborda la amenaza del robo de información de la cuenta de pago a través de los sistemas comerciales. Para hacerlo, D1 introduce un sistema de gestión de transacciones con información de cuenta de pago almacenada y busca evitar la captura de información de la cuenta de pago de las tarjetas de pago en un dispositivo POS de un sistema comercial durante una transacción. La presente invención (cuando se aplica a pagos), por otro lado, aborda la amenaza de mal manejo y uso indebido de

	tarjetas / dispositivos de pago (como documentos legibles por máquina) que contienen información de cuenta de pago (como grupo de credenciales) en un dispositivo POS (como dispositivo de aceptación / punto final de red). Para hacer esto, la presente invención, a diferencia de D1, busca permitir la captura de una lectura de un documento legible por máquina en un punto final de red durante una interacción solo si está permitido por el titular legítimo del documento.
La diferencia entre la invención, definida en la reivindicación 25 y el método de D1 consiste en que en el método de la Reivindicación 1 incluye una etapa de búsqueda de un código secreto que es conocido entre dos partes para completar la transacción.	D1 no enseña varias características de la presente invención, que incluyen, pero no se limitan a, al menos, las características que implican un servidor de control con un par de dispositivos de control de la Reivindicación 1 descritas en los puntos (i), (ii), y (iii).
El efecto que logra la inclusión de una etapa de búsqueda de un código secreto que es conocido entre dos partes para completar la transacción es garantizar la confiabilidad y seguridad de los datos intercambiados durante la transacción.	El efecto logrado al incluir la búsqueda del código secreto no es garantizar la fiabilidad y seguridad de la información intercambiada durante la transacción. En cambio, el efecto logrado al incluir la búsqueda del código secreto que es: - conocido solo por el presentador [párrafo 0044]); - obtenido en un dispositivo aceptante correspondiente a un punto final de red; - vinculado en un servidor a un identificador de presentador correspondiente a un titular legítimo de un documento legible por máquina; es garantizar el permiso del titular legítimo del documento para capturar una lectura en el punto final de red.
Por lo tanto, el problema técnico objetivo que pretende resolver esta invención se puede formular así: <i>"¿cómo modificar el método conocido en D1 para garantizar la confiabilidad y seguridad de los datos intercambiados durante la transacción?"</i> .	El problema técnico objetivo que la presente invención pretende resolver no puede ser formulado por el examinador sobre la base de D1. En cambio, el problema técnico objetivo que la presente invención intenta resolver es <i>"cómo controlar la captura de una lectura de un documento legible por máquina en un punto final de red durante una interacción con el fin de garantizar el permiso del titular legítimo del documento para que una lectura sea capturada en el punto final de la red"</i> .
Sin embargo, la inclusión de una etapa de búsqueda de un código secreto que es conocido entre dos partes, ya está divulgada en el documento D2 que se refiere a que el servidor (30) responde (en el paso (120)) a dicha llamada telefónica de voz solicitando al cliente (es decir, la persona que maneja dicho teléfono móvil (10)) que valide la transacción electrónica mediante un código PIN de validación (en los dibujos adjuntos mencionados en un breve formulario como "PIN de validación"), que también está memorizado en la base de datos (31) del servidor (30); (...) El código PIN de validación está disponible solo para el usuario autorizado del teléfono y no puede ser conocido por un ladrón que ha robado un teléfono móvil ya encendido y para el cual la barrera de protección constituida por los códigos PIN del teléfono ya se ha superado (Pág. 5, Lí. 25).	D2 comienza con la captura de información de identificación en un POS como se describe en el paso 100 <i>"iniciar una transacción electrónica que transmite información de identificación inalámbrica desde un módulo de pago electrónico (11) de un teléfono móvil (10) a un POS (20), que reenvía dicha información de identificación junto con los datos de transacción a una red minorista (21) y a un servidor (30), ..."</i> Después de la captura de la información de identificación, un PIN de validación se proporciona por separado <i>"vocalmente"</i> o <i>"textualmente"</i> a dicho servidor que tiene un efecto de control en el procesamiento de transacciones. Esto es distinto de un código clave secreto en la Reivindicación 1 que tiene un efecto de control en la captura de una lectura de un documento legible por máquina en un punto final de red antes de que pueda comenzar una transacción (si la hay).

En consecuencia, la persona del oficio normalmente versada en la materia incluiría la etapa de búsqueda de un código secreto que es conocido entre dos partes para completar la transacción mencionada en el documento D2 en el método divulgado en el documento D1 para llegar así al objeto de la Reivindicación 1 de la solicitud. Por lo cual se considera obvia.	En consecuencia, el objeto de la Reivindicación 1 de la presente invención no puede lograrse cuando un PHOSITA incluye la etapa de búsqueda de un código secreto de D2 en el sistema descrito en D1. Como tal, la Reivindicación 1 no es obvia.
---	---

Además, respetuosamente quiero mencionar que D1 y D2 fueron también mencionados en el Reporte Preliminar de Patentabilidad Internacional (IPRP) y que las objeciones por nivel inventivo fueron superados al mencionar las diferencias enumeradas en este memorial, lo cual resulto en la concesión de patente para las solicitudes equivalentes en Europa (Patente No. EP3092774B1) y en Estados Unidos (Patente No. US10021093B2). Ahora bien, a pesar de que las concesiones en otras jurisdicciones no tienen un carácter vinculante que obligue a la Superintendencia de Industria y Comercio (SIC) a conceder una patente en Colombia, es importante resaltar que los estándares de patentabilidad son semejantes a nivel mundial y las concesiones en otros países sí dan luces e indicios de la patentabilidad de una invención, como sucede en el presente caso.

Así las cosas, la Guía de la SIC establece que las invenciones carecen de nivel inventivo cuando “(...) en el estado de la técnica en su conjunto hay un segundo documento que contiene una enseñanza que indicaría (no sólo que podría indicar, sino que indicaría) a la persona medianamente versada en la materia, enfrentada al problema técnico, cómo modificar o adaptar el estado de la técnica más cercano para resolver el problema, de la forma reivindicada, sin realizar una actividad inventiva”.¹ En el presente caso, es evidente que las características técnicas esenciales de la invención no se podían prever a partir de las enseñanzas del arte previo citado por el Examinador sin llevar a cabo actividad inventiva.

Por las razones expuestas anteriormente, considero que la Reivindicación 25 también es inventiva, pues contiene también las características esenciales que diferencian a la Reivindicación 1 con D1 y D2. Además, considero que las Reivindicaciones 2 a 24 y 26 a 36 también son inventivas ya que al ser dependientes de la Reivindicación 1 o de la

¹ Oficina Internacional de la OMPI, *Manual para el Examen de Solicitudes de Patente de Invención en las Oficinas de Propiedad Industrial de los Países de la Comunidad Andina* (Quito, Ecuador, 2004) Sección 2.13.5.1

Reivindicación 25, presentan todas y cada una de sus características técnicas y, por lo tanto, presentan nivel inventivo.

En conclusión, según la aproximación problema-solución para el análisis del nivel inventivo de la presente invención, considero que éste se reconoce claramente, ya que, puesto que el arte previo en efecto no es suficiente para brindar indicaciones acerca de la posibilidad de desarrollar la invención de manera evidente, la persona del oficio normalmente versada en la materia reconocería que la presente invención es inventiva.

V. PETICIÓN

Puesto que se ha dado respuesta a todas las objeciones formuladas por la Dirección de Nuevas Creaciones, se solicita proceder al otorgamiento de la solicitud de patente.

VI. ENTREVISTA CON EL EXAMINADOR

Además de este memorial de respuesta he solicitado una entrevista en las oficinas de la Dirección de Nuevas Creaciones con el fin de discutir con el Examinador temas que considero de importancia para el trámite. Atentamente solicito no se resuelva este expediente hasta después de llevar a cabo dicha reunión.

VII. ANEXOS

1. Capítulo Reivindicatorio Modificado conformado por 36 reivindicaciones.

Señor Director,

ANDRÉS RINCÓN USCÁTEGUI
C.C. 79.780.910 de Bogotá
T.P. 114.908