

PROTECCIÓN CONTRA COMPARTICIÓN PARA UNA EXPERIENCIA DE COMPARTICIÓN DE LA PANTALLA

Antecedentes de la invención

5 Los sistemas de comunicación modernos tienen una serie de capacidades, que incluyen la integración de diversos modos de comunicación con diferentes servicios. Por ejemplo, mensajería instantánea, comunicaciones de voz/video, compartición de datos/aplicaciones, uso de pizarra electrónica y otras formas de comunicación pueden combinarse con la información de presencia y disponibilidad para los suscriptores. Tales sistemas pueden proporcionar a los suscriptores capacidades mejoradas, como proporcionar instrucciones a los interlocutores para varias categorías de estado, contactos alternativos, información de calendario y funciones comparables. Además, los sistemas de colaboración que permiten a los usuarios compartir y colaborar en la creación y modificación de diversos tipos de documentos y contenido pueden integrarse con los sistemas de comunicación multimodales que proporcionan diferentes tipos de capacidades de comunicación y colaboración. Tales sistemas integrados ocasionalmente se denominan sistemas de comunicación y colaboración unificadas (UC&C, por sus siglas en inglés).

Aunque los sistemas UC&C proporcionan una mayor flexibilidad en las comunicaciones, también presentan una serie de desafíos de implementación. Por ejemplo, un usuario puede desear compartir el contenido de la pantalla con diferentes dispositivos que participan en la comunicación UC&C. Sin embargo, el usuario puede desear proteger parte del contenido de la pantalla para que no se comparta. La habilitación de la compartición de pantalla y de la protección de contenido simultáneos presenta varios desafíos de implementación.

Breve descripción de la invención

Esta breve descripción de la invención se proporciona para introducir una selección de conceptos en una forma simplificada, los cuales se describen posteriormente con más detalle en la descripción detallada. Esta breve descripción de la invención no se propone para identificar las características importantes o las características esenciales de la materia objeto reivindicada, ni pretende utilizarse como un auxiliar en la determinación del alcance de la materia objeto reivindicada.

Se describen técnicas para la protección contra compartición para una experiencia de compartición de pantalla. En al menos algunas modalidades, una experiencia de compartición de pantalla implica que un usuario comparta porciones de su pantalla de presentación con otros usuarios como parte de una sesión de comunicación. De acuerdo con varias modalidades, un usuario que comparte su pantalla con otros dispositivos como parte de una experiencia de compartición de pantalla puede evitar que una porción de la pantalla se comparta al designar la porción como protegida contra compartición. Por lo tanto, el contenido de la porción identificada de la pantalla del usuario se cifra para que otros dispositivos que no pueden descifrar el contenido no puedan visualizarlo. De acuerdo con una o más modalidades, a un usuario puede designársele permisos de tal manera que el usuario pueda tener acceso a una clave de cifrado para descifrar y visualizar la porción protegida contra compartición como parte de una experiencia de

compartición de pantalla.

Breve descripción de los dibujos

La descripción detallada se presenta con referencia a las figuras adjuntas. En las figuras, los dígitos extremos izquierdos de un número de referencia identifican la figura en la cual aparece por primera vez el número de referencia. El uso de los mismos números de referencia en diferentes casos en la descripción y en las figuras puede indicar elementos similares o idénticos. Los números idénticos seguidos por letras diferentes en un número de referencia pueden referirse a los diferentes casos de un elemento particular.

La figura 1 es una ilustración de un entorno en una implementación ejemplar que es operable para emplear las técnicas abordadas en el presente documento.

La figura 2 representa un caso de implementación ejemplar para proteger contenido durante una experiencia de compartición de pantalla de acuerdo con una o más modalidades.

La figura 3 representa un caso de implementación ejemplar para proteger contenido durante una experiencia de compartición de pantalla de acuerdo con una o más modalidades.

La figura 4 muestra un caso de implementación ejemplar para permitir que un usuario autorizado pueda acceder al contenido protegido contra compartición durante una experiencia de compartición de pantalla de acuerdo con una o más modalidades.

La figura 5 representa un caso de implementación ejemplar para designar una región protegida contra compartición de acuerdo con una o más modalidades.

La figura 6 representa un caso de implementación ejemplar para designar una región protegida contra compartición de acuerdo con una o más modalidades.

La figura 7 representa un caso de implementación ejemplar para designar un conjunto de usuarios que tiene permitido visualizar una región protegida contra compartición de acuerdo con una o más modalidades.

La figura 8 representa un caso de implementación ejemplar para designar usuarios que están autorizados para la compartición de acuerdo con una o más modalidades.

La figura 9 es un diagrama de flujo que describe las etapas en un método para controlar el acceso al contenido de una región protegida contra compartición de acuerdo con una o más modalidades.

La figura 10 es un diagrama de flujo que describe las etapas en un método para controlar el acceso al contenido de una región protegida contra compartición de acuerdo con una o más modalidades.

La figura 11 es un diagrama de flujo que describe las etapas en un método para ocultar visualmente una región protegida contra compartición de acuerdo con una o más modalidades.

La figura 12 ilustra un sistema y un dispositivo informático ejemplares tal como se describe con referencia a la figura 1, que están configurados para implementar las modalidades de las técnicas descritas en el presente documento.

Descripción detallada de la invención

Se describen las técnicas para la protección contra compartición para una experiencia de

compartición de pantalla. En al menos algunas implementaciones, una experiencia de compartición de pantalla implica que un usuario comparta porciones de su pantalla de presentación con otros usuarios como parte de una sesión de comunicación. Una sesión de comunicación, por ejemplo, se refiere a un intercambio en tiempo real de medios de comunicación entre diferentes terminales de comunicación. Los ejemplos de una sesión de comunicación incluyen una llamada de voz mediante el protocolo de transmisión de la voz por internet (VoIP, por sus siglas en inglés), videollamada, mensajería de texto, transferencia de archivos, compartición de contenido y/o combinaciones de los mismos. En al menos una implementación, una sesión de comunicación representa una sesión de comunicación y colaboración unificadas (UC&C, por sus siglas en inglés).

De acuerdo con diversas implementaciones, un usuario que comparte su pantalla con otros dispositivos como parte de una experiencia de compartición de pantalla desea proteger una porción de la pantalla contra compartición. Por ejemplo, una porción de su pantalla puede presentar información confidencial y/o personal que el usuario no desea compartir. Por consiguiente, el usuario activa una funcionalidad de protección contra compartición para permitir al usuario identificar una porción de su pantalla como que no debe compartirse con los otros dispositivos. El usuario, por ejemplo, puede establecer una zona de protección alrededor de una porción de su pantalla que desea compartir. A continuación, se describen otras formas de designar una porción particular de una pantalla de presentación como protegida contra compartición. Por lo tanto, la porción identificada de la pantalla del usuario se cifra, mientras otras porciones se comparten sin obstáculos como parte de la experiencia de compartición de pantalla.

De acuerdo con una o más implementaciones, a un usuario puede asignársele la autorización, de modo que se le permita al usuario visualizar el contenido que se designa como protegido contra compartición como parte de una experiencia de compartición de pantalla. Por ejemplo, un usuario de compartición que especifica una porción de su pantalla de presentación como protegida contra compartición como parte de una experiencia de compartición de pantalla, puede identificar a un participante en la experiencia de compartición de pantalla como autorizado para la compartición. Por lo tanto, un dispositivo asociado con el participante autorizado tiene acceso a una clave de cifrado de tal manera que el dispositivo pueda descifrar el contenido de la porción protegida contra compartición de pantalla y presentar el contenido descifrado sin obstáculos. Sin embargo, otros participantes no autorizados en la experiencia de compartición de pantalla, no tienen acceso a la clave de cifrado y, por lo tanto, no pueden descifrar ni visualizar el contenido protegido. De esta manera, un usuario puede proteger cierto contenido de la pantalla contra compartición general, a la vez que designa un conjunto de usuarios autorizados que tienen permiso para visualizar el contenido.

Por consiguiente, las técnicas de la protección contra compartición para una experiencia de compartición de pantalla descritas en el presente documento mejoran la capacidad de los usuarios para proteger el contenido y los datos confidenciales durante una experiencia de compartición de pantalla, de tal modo mejorando la seguridad de los datos para los datos confidenciales del usuario y evitando la exposición no deseada de contenido confidencial del usuario. Las técnicas descritas también mejoran el rendimiento del dispositivo informático durante una experiencia de compartición de pantalla al permitir que

las claves de cifrado que descifran el contenido protegido se distribuyan de manera eficiente a los dispositivos autorizados.

En el siguiente análisis, primero se describe un entorno ejemplar que es operable para emplear las técnicas descritas en el presente documento. A continuación, algunos casos de implementación ejemplares se describen de acuerdo con una o más modalidades. A continuación, se describen algunos procedimientos ejemplares de acuerdo con una o más modalidades. Finalmente, se describen un sistema y dispositivo ejemplares que son operables para emplear las técnicas abordadas en el presente documento de acuerdo con una o más modalidades. Ahora se considera un entorno ejemplar en el cual pueden emplearse las implementaciones ejemplares.

La figura 1 es una ilustración de un entorno 100 en una implementación ejemplar que es operable para emplear las técnicas de protección contra compartición para una experiencia de compartición de pantalla descrita en el presente documento. En general, el entorno 100 incluye varios dispositivos, servicios y redes que permiten la comunicación a través de una variedad de modalidades diferentes. Por ejemplo, el entorno 100 incluye un dispositivo cliente 102 conectado a una red 104. El dispositivo cliente 102 puede configurarse de varias maneras, como una computadora tradicional (por ejemplo, una computadora personal de escritorio, computadora portátil, etcétera), estación móvil, dispositivo de entretenimiento, teléfono inteligente, dispositivo portátil, minicomputadora portátil, consola de videojuegos, dispositivo portable (por ejemplo, una tableta), etcétera.

La red 104 es representativa de una red que proporciona conectividad al dispositivo cliente 102 a varias redes y/o servicios, como internet. La red 104 puede proporcionar al dispositivo cliente 102 conectividad a través de una variedad de diferentes tecnologías de conectividad, como cable de banda ancha, línea de suscriptor digital (DSL, por sus siglas en inglés), conectividad celular inalámbrica, conectividad de datos inalámbrica (por ejemplo, *WiFi*[™]), portadora T (por ejemplo, T1), Ethernet, etcétera. En al menos algunas implementaciones, la red 104 representa diferentes redes alámbricas e inalámbricas interconectadas.

El dispositivo cliente 102 incluye una variedad de funcionalidades diferentes que permiten realizar diversas actividades y tareas. Por ejemplo, el dispositivo cliente 102 incluye un sistema operativo 106, aplicaciones 108, cliente de comunicación 110 y módulo de comunicación 112. En general, el sistema operativo 106 es representativo de la funcionalidad para extraer varios componentes del sistema del dispositivo cliente 102, como *hardware*, módulos y servicios a nivel de núcleo, etcétera. El sistema operativo 106, por ejemplo, puede extraer varios componentes del dispositivo cliente 102 para las aplicaciones 108 a modo de permitir la interacción entre los componentes y las aplicaciones 108.

Las aplicaciones 108 representan funcionalidades para realizar diferentes tareas a través del dispositivo cliente 102. Los ejemplos de las aplicaciones 108 incluyen una aplicación de procesamiento de textos, aplicación de hoja de cálculo, navegador web, aplicación de juegos, etcétera. Las aplicaciones 108 pueden instalarse localmente en el dispositivo cliente 102 para ejecutarse a través de un entorno de ejecución local, y/o pueden representar portales para funcionalidades remotas, como servicios con base en la nube, aplicaciones web, etcétera. Por lo tanto, las aplicaciones 108 pueden adoptar una variedad de

formas, como código ejecutado localmente, portales a servicios alojados remotamente, etcétera.

El cliente de comunicación 110 es representativo de la funcionalidad para permitir diferentes formas de comunicación a través del dispositivo cliente 102. Los ejemplos del cliente de comunicación 110 incluyen una aplicación de comunicación por voz (por ejemplo, un cliente de VoIP), aplicación de comunicación por video, aplicación de mensajería, aplicación de compartición de contenido, aplicación de comunicación y colaboración unificadas (UC&C, por sus siglas en inglés) y combinaciones de las mismas. El cliente de comunicación 110, por ejemplo, permite combinar diferentes modalidades de comunicación para proporcionar diversos casos de comunicación.

El módulo de comunicación 112 es representativo de la funcionalidad para permitir que el dispositivo cliente 102 comunique datos a través de conexiones alámbricas y/o inalámbricas. Por ejemplo, el módulo de comunicación 112 representa el *hardware* y la lógica para la comunicación de datos a través de una variedad de diferentes tecnologías y protocolos alámbricos y/o inalámbricos.

El dispositivo cliente 102 incluye, además, un dispositivo de presentación 114, que representa la funcionalidad para la salida visual para el dispositivo cliente 102. Además, el dispositivo de presentación 114 representa la funcionalidad para recibir varios tipos de entrada, como entrada táctil, entrada de lápiz, etcétera.

El entorno 100 incluye, además, dispositivos terminales 116, que son representativos de dispositivos y/o funcionalidades con los cuales puede comunicarse el dispositivo cliente 102. En al menos algunas implementaciones, los dispositivos terminales 116 representan dispositivos de usuario final como los abordados con referencia al dispositivo cliente 102. Los dispositivos terminales 116 incluyen clientes de comunicación 118, que son representativos de funcionalidades para permitir diferentes formas de comunicación a través de los dispositivos terminales 116. Los clientes de comunicación 118, por ejemplo, representan diferentes instancias del cliente de comunicación 110. Para los propósitos de análisis en el presente documento, se hace referencia a un dispositivo terminal 116 y un cliente de comunicación 118, que representan ejemplos de los dispositivos terminales 116 y clientes de comunicación 118, respectivamente.

En al menos algunas implementaciones, los clientes de comunicación 110, 118 representan las interfaces para un servicio de comunicación 120. En general, el servicio de comunicación 120 es representativo de un servicio para realizar diversas tareas para la gestión de la comunicación entre el dispositivo cliente 102 y el dispositivo terminal 116. El servicio de comunicación 120, por ejemplo, puede gestionar la iniciación, moderación y terminación de las sesiones de comunicación entre los clientes de comunicación 110, 118.

El servicio de comunicación 120 mantiene una presencia en muchas redes diferentes y puede implementarse de acuerdo con una variedad de arquitecturas diferentes, como un servicio basado en la nube, servicio distribuido, servicio basado en la web, etcétera. Los ejemplos del servicio de comunicación 120 incluyen un servicio de VoIP, servicio de conferencia en línea, servicio de UC&C, etcétera.

El cliente de comunicación 110 incluye, además, un módulo de compartición 122, que es representativo de la funcionalidad para realizar diversos aspectos de las técnicas para la protección contra

compartición para una experiencia de compartición de pantalla analizada en el presente documento. A continuación, se detallan varios atributos y aspectos operativos del módulo de compartición 122. El módulo de compartición 122 mantiene las políticas de compartición 124, que son representativas de diferentes conjuntos de datos que especifican permisos y criterios para intercambiar contenido entre el dispositivo cliente 102 y los dispositivos terminales 116. Las políticas de compartición 124, por ejemplo, especifican qué regiones del dispositivo de presentación 114 pueden compartirse con los dispositivos terminales 116, y qué regiones del dispositivo de presentación 114 no pueden compartirse con los dispositivos terminales 116. Además, o como una alternativa, las políticas de compartición 124 son específicas para el contenido y/o la aplicación. Por ejemplo, las políticas de compartición 124 pueden especificar ciertos tipos de contenido que pueden compartirse con los dispositivos terminales 116, y otros tipos de contenido que no pueden compartirse con los dispositivos terminales 116. Además, las políticas de compartición 124 pueden especificar que una ventana de aplicación para una aplicación particular 108 puede compartirse, mientras una ventana de aplicación para una aplicación diferente 108 no puede compartirse. En general, las políticas de compartición 124 pueden configurarse de varias maneras, como a través de la configuración predeterminada especificada por parte de un desarrollador de aplicaciones, configuración especificada por parte del usuario final, por parte del personal de tecnología de la información (TI, por sus siglas en inglés), etcétera.

El cliente de comunicación 110, además, mantiene y/o tiene acceso adicional a miembros de grupo 126, que representan identificadores para grupos diferentes de los que es miembro un usuario 128 del dispositivo cliente 102. En general, un “grupo” se refiere a una agrupación de diferentes usuarios con base en diferentes criterios. Un grupo particular, por ejemplo, representa una serie de identificadores de usuario y/o identificadores de dispositivos que pertenecen al grupo particular. En general, puede crearse y administrarse un grupo para controlar el acceso a los recursos de *hardware*, recursos de *software*, contenido, sistemas de archivos (por ejemplo, directorios), etcétera. Los ejemplos de un grupo incluyen un grupo de usuarios, grupo de correo electrónico, grupo de directorios, etcétera. Al menos en algunas implementaciones, las políticas de compartición 124 identifican grupos autorizados específicos con los cuales una región protegida contra compartición puede compartirse “sin obstáculos”. En general, el término “sin obstáculos”, tal como se utiliza en el presente documento, se refiere a la capacidad de visualizar el contenido en forma no cifrada y/o no oculta, tal como se habilita mediante el descifrado de contenido cifrado. Por ejemplo, una política de compartición 124 particular puede especificar que contenido protegido contra compartición puede compartirse con un grupo particular, pero no debe compartirse con usuarios fuera del grupo particular, por ejemplo, usuarios que no son miembros del grupo particular. Además, o como una alternativa a la designación de grupos con autorización de compartición, las políticas de compartición 124 pueden designar a los usuarios, dispositivos, dominios de red, etcétera, específicos autorizados para la compartición.

Aunque el módulo de compartición 122 y las políticas de compartición 124 se representan como implementadas en el dispositivo cliente 102, debe apreciarse que, en algunas implementaciones adicionales o alternativas, la funcionalidad del módulo de compartición 122 y/o las políticas de compartición

124 pueden implementarse de manera parcial o completa a través de un servicio basado en la red, como el servicio de comunicación 120. Por ejemplo, el servicio de comunicación 120 puede realizar varios aspectos de las técnicas para la protección contra compartición para una experiencia de compartición de pantalla descrita en el presente documento.

5 El dispositivo cliente 102 incluye, además, un módulo de cifrado 130 y un códec 132. El módulo de cifrado 130 es representativo de la funcionalidad para cifrar y descifrar los datos, como para cifrar el contenido de la pantalla como parte de una experiencia de compartición de pantalla. Para al menos este propósito, el módulo de cifrado 130 incluye y/o tiene acceso a las claves de cifrado ("claves") 134, que son representativas de las claves que pueden utilizarse para cifrar y descifrar la información. Las claves 134, por ejemplo, pueden utilizarse por el módulo de cifrado 130 para cifrar el contenido protegido contra compartición. El contenido protegido contra compartición, por ejemplo, puede cifrarse por el módulo de cifrado 130, de manera que un dispositivo terminal 116 que recibe el contenido cifrado no pueda visualizar el contenido sin obstáculos a menos que el dispositivo terminal 116 tenga acceso a una clave particular 134 que se utilizó para cifrar el contenido.

15 En al menos algunas implementaciones, el módulo de cifrado 130 puede incluir una función de aleatorización (por ejemplo, un aleatorizador) que codifica el contenido protegido contra compartición para evitar que el contenido protegido se visualice sin obstáculos. Por ejemplo, el módulo de cifrado 130 puede aplicar un algoritmo de aleatorización y/u otra técnica de aleatorización de datos para aleatorizar los datos del contenido protegido contra compartición y evitar que otros dispositivos accedan al contenido protegido. Tal como se utiliza en el presente documento, el cifrado puede referirse al cifrado que codifica los datos con una clave, a la aleatorización que codifica los datos utilizando un algoritmo de aleatorización, y/o combinaciones de los mismos.

25 El códec 132 es representativo de la funcionalidad para codificar y decodificar el contenido, como para codificar y decodificar una emisión en continuo de contenido (por ejemplo, que incluye video, audio, archivos, etcétera) que se genera como parte de una experiencia de compartición de pantalla. El códec 132, por ejemplo, está configurado para realizar la compresión y descompresión de los datos de contenido, tal como para reducir el ancho de banda de transmisión requerido para transmitir una emisión en continuo de contenido como parte de una experiencia de compartición de pantalla.

30 Una vez que se describió un entorno ejemplar en el cual pueden operar las técnicas descritas en el presente documento, ahora se considera un análisis de un caso de implementación ejemplar para la protección contra compartición para una experiencia de compartición de pantalla de acuerdo con una o más modalidades.

35 La siguiente sección describe algunos casos de implementación ejemplares de la protección contra compartición para una experiencia de compartición de pantalla de acuerdo con una o más implementaciones. Los casos de implementación pueden implementarse en el entorno 100 abordado anteriormente, y/o cualquier otro entorno adecuado.

La figura 2 muestra un caso de implementación 200 ejemplar para proteger el contenido durante una experiencia de compartición de pantalla de acuerdo con una o más implementaciones. El caso 200

incluye varias entidades y componentes introducidos anteriormente con referencia al entorno 100.

En el caso 200, el usuario 128 del dispositivo cliente 102 está involucrado en una sesión de comunicación 204 con un usuario 202 de un dispositivo terminal 116a. En general, la sesión de comunicación 204 representa un intercambio en tiempo real de diferentes medios de comunicación entre el dispositivo cliente 102 y el dispositivo terminal 116a, como audio, video, archivos, contenido multimedia y/o combinaciones de los mismos. En este ejemplo particular, la sesión de comunicación 204 implica un intercambio en tiempo real de datos de voz 206 y datos de video 208 entre el dispositivo cliente 102 y el dispositivo terminal 116a a través de la red 104.

Como parte de la sesión de comunicación 204, el usuario 128 realiza una acción para compartir una porción de un escritorio 210 del dispositivo de presentación 114 con el usuario 202. En general, el escritorio 210 representa una porción del dispositivo de presentación 114 en la cual se presentan diferentes interfaces y controles para aplicaciones, tareas, operaciones de sistema, etcétera. Por ejemplo, el usuario 128 selecciona un control de compartición 212 desde una interfaz de cliente de comunicación 214a. En general, la interfaz de cliente de comunicación 214a representa una interfaz para el cliente de comunicación 110 que permite al usuario 128 realizar varias acciones y visualizar la información de estado perteneciente a la sesión de comunicación 204. La selección del control de compartición 212 activa un modo de compartición 216 que causa que al menos una porción del escritorio 210 se comparta con el dispositivo terminal 116a.

Por consiguiente, en respuesta a la acción del usuario para activar el modo de compartición 216, una región 218a del escritorio 210 se comparte con el dispositivo terminal 116a. La acción del usuario para compartir el escritorio 210 provoca que se presente una representación visual 220 de la región 218a dentro de una interfaz de cliente de comunicación 214a presentada en un visualizador 222 del dispositivo terminal 116a. La representación visual 220, por ejemplo, representa una copia en directo de la región 218a que se comunica desde el dispositivo cliente 102 al dispositivo terminal 116a como parte de los datos de video 208. En general, la interfaz de cliente de comunicación 214a representa una GUI del cliente de comunicación 118.

Cabe destacar que, aunque la región 218a se comparte con el dispositivo terminal 116a, una región diferente 218b del escritorio 210 no se comparte con el dispositivo terminal 116a. De acuerdo con las técnicas de protección contra compartición para una experiencia de compartición de pantalla descrita en el presente documento, la región 218b se designa como una región protegida que no debe compartirse con el dispositivo terminal 116a. En general, la región 218b puede designarse como una región protegida de varias maneras, como, mediante una acción del usuario que identifica a la región 218b como una región protegida. Por ejemplo, el usuario 128 selecciona un control de protección 224 en la interfaz de cliente de comunicación 214a, que activa un modo de protección contra compartición que permite que la región 218b se designe como protegida contra compartición. A continuación, se abordan los ejemplos de diferentes formas de designar las regiones protegidas de un área de presentación.

Para permitir que la región 218b se proteja contra la compartición con el dispositivo terminal 116a, el cliente de comunicación 110 se interconecta con el módulo de cifrado 130 para provocar que la región

218b se cifre, como utilizando una clave 134a. Por ejemplo, el módulo de compartición 122 transmite un identificador (ID, por sus siglas en inglés) de región 226 para la región 218b al módulo de cifrado 130, y el módulo de cifrado 130 cifra los datos de la región 218b utilizando la clave 134a para generar los datos de video cifrados 228. En general, el ID de región 226 puede implementarse de varias maneras, como las

5 coordenadas de píxeles que definen la región 218b, un identificador de aplicación para una aplicación 108 que presenta el contenido dentro de la región 218b, un identificador de archivo para el contenido presentado dentro de la región 218b, etcétera.

Por consiguiente, los datos de video cifrados 228 pueden comunicarse con el flujo de datos de la sesión de comunicación 204. Sin embargo, dado que el dispositivo terminal 116a no tiene acceso a la clave

10 134a, el dispositivo terminal 116a no puede descifrar los datos de video cifrados 228 ni mostrar sin obstáculos el contenido de la región 218b.

De esta manera, diferentes regiones de un área de presentación (por ejemplo, un escritorio) pueden definirse con compartición restringida para permitir que se compartan algunas porciones de un visualizador, y otras porciones se protejan contra compartición. En general, el contenido puede designarse como

15 protegido contra compartición de forma dinámica al mismo tiempo que la sesión de comunicación 204 está en progreso. Por ejemplo, el usuario 128 puede realizar acciones para provocar que la protección contra compartición para la región 218b se aplique y después se elimine al mismo tiempo que la sesión de comunicación 204 está en progreso. Además, o como una alternativa, cierto contenido puede designarse de forma persistente como protegido contra compartición, de modo que la protección contra compartición

20 se aplique automáticamente a través de múltiples sesiones de comunicación separadas. La protección contra compartición persistente, por ejemplo, puede aplicarse con base en un ID de aplicación, tipo de contenido, porción específica del escritorio 210, etcétera.

La figura 3 muestra un caso de implementación 300 ejemplar para proteger el contenido durante una experiencia de compartición de pantalla de acuerdo con una o más implementaciones. El caso 300

25 incluye varias entidades y componentes introducidos anteriormente con referencia al entorno 100. En al menos algunas implementaciones, el caso 300 representa una continuación y/o variación del caso 200 descrito anteriormente.

En el caso 300, el usuario 128 participa en una experiencia de compartición de pantalla con un usuario 302 como parte de la sesión de comunicación 204, y designa a la región 218b como protegida

30 contra compartición, tal como se describe en otra parte en el presente documento. En respuesta, el módulo de cifrado 130 cifra el contenido en la región 218b. Sin embargo, en este caso particular, el contenido en la región 218b está cifrado localmente, de manera que el contenido se oculta tanto en el visualizador 114 como en el visualizador 304 de un dispositivo terminal 116b del usuario 302. Por ejemplo, cabe destacar que la región 218b está visualmente oculta (por ejemplo, aleatorizada) en el escritorio 210, así como en

35 una interfaz de cliente de comunicación 214b presentada por un cliente de comunicación 118b del dispositivo terminal 116b. En al menos algunas implementaciones, el hecho de ocultar visualmente la región 218b localmente en el escritorio 210 permite que todo el escritorio 210 se capture y codifique por el códec 132 y se transmita al dispositivo terminal 116c como un único flujo de video codificado 304. Por ejemplo, el

flujo de video codificado 304 incluye datos de video 306 y datos de voz 306, y los datos de video 306 incluyen porciones no ocultas (por ejemplo, sin cifrar) del escritorio 210 (por ejemplo, la región 218a) así como la región oculta 218b. Por lo tanto, todo el escritorio 210 puede transmitirse como parte de la sesión de comunicación 204 sin requerir que la región 218b se cifre y comunique como una porción de contenido cifrada por separado como parte de la sesión de comunicación 204.

La figura 4 representa un caso de implementación 400 ejemplar para permitir que un usuario autorizado pueda acceder al contenido protegido contra compartición durante una experiencia de pantalla compartida de acuerdo con una o más implementaciones. El caso 400 incluye varias entidades y componentes introducidos anteriormente con referencia al entorno 100. En al menos algunas implementaciones, el caso 400 representa una continuación y/o variación de los casos 200, 300 descritos anteriormente.

En el caso 400, el usuario 128 participa en una experiencia de compartición de pantalla con un usuario 402 como parte de la sesión de comunicación 204, y designa a la región 218b como protegida contra compartición, tal como se describe en otra parte en el presente documento. En respuesta, el módulo de cifrado 130 cifra el contenido de la región 218b con una clave de cifrado 134c para generar los datos de video cifrados 404. Por lo tanto, los datos de video cifrados 404 se transmiten a un dispositivo terminal 118c del usuario 402 junto con los datos de voz 206 y los datos de video 208.

En este caso particular, un dispositivo terminal 116c incluye y/o tiene acceso a una clave 406, que representa una instancia de la clave 134c utilizada para cifrar los datos de video cifrados 404. En consecuencia, el dispositivo terminal 116c puede descifrar el cifrado los datos de video 404 para permitir una representación visual 408 del escritorio 210 que se presentará, que incluye el contenido de la región 218a y de la región 218b sin obstáculos como parte de una interfaz de cliente de comunicaciones 214c para un cliente de comunicaciones 118c. Otros dispositivos terminales 116 que participan en la sesión de comunicación 204 que no tienen acceso a la clave 406 pueden recibir los datos de video cifrados 404, pero no podrán descifrar los datos cifrados 404 y visualizar sin obstáculos la región 218b.

En general, el dispositivo terminal 116c puede tener acceso a la clave 406 de varias maneras. Por ejemplo, la clave 406 puede comunicarse al dispositivo extremo 116c junto con una invitación para participar en la sesión de comunicación 204, como integrada y/o adjunta en la invitación. Como otro ejemplo, la clave 406 puede comunicarse al dispositivo terminal 116c separada de una invitación, como parte de un correo electrónico, en un mensaje instantáneo, un mensaje de texto, etcétera.

En una implementación ejemplar, la clave 406 puede ser accesible para el dispositivo terminal 116c debido a que el usuario 128 es miembro de un grupo autorizado que tiene derecho a acceder a la clave 406. Por ejemplo, la membresía en un grupo común da derecho a sus usuarios a acceder a la clave 406, y los usuarios fuera de ese grupo que no están designados específicamente como autorizadas para la compartición no tienen derecho a acceder a la clave 406. En al menos algunas implementaciones, la clave 406 está disponible para el dispositivo terminal 116c debido a que el usuario 402 y el usuario 128 son miembros del mismo grupo. Por ejemplo, los permisos grupales para que el grupo de derecho a sus miembros a acceder a la clave 406.

La figura 5 muestra un caso de implementación ejemplar 500 para designar una región protegida contra compartición de acuerdo con una o más implementaciones. El caso 500 incluye varias entidades y componentes introducidos anteriormente con referencia al entorno 100. En al menos algunas implementaciones, el caso 500 representa una continuación y/o variación de los casos 200-400 descritos anteriormente.

En el caso 500, el dispositivo cliente 102 está en el modo de compartición 216. Además, el usuario 128 designa a la región 218b como una región protegida contra compartición, por lo cual la región 218b no se comparte con otro dispositivo mientras el modo de compartición 216 esté activo, tal como se describió en los casos anteriores. El usuario 128, por ejemplo, utiliza la entrada táctil en el dispositivo de presentación 114 para delinear una zona de protección 502 alrededor de la región 218b. También pueden utilizarse otros tipos de entrada para delinear la zona de protección 502, como entrada con ratón y cursor, entrada con gestos sin contacto, entrada de lápiz, etcétera. En este ejemplo particular, la zona de protección 502 se indica visualmente a través de una línea discontinua para proporcionar una disponibilidad visual de una parte del dispositivo de presentación 114 que se designa como protegida contra compartición.

En al menos una implementación, el usuario 128 activa un modo de protección contra compartición (SP, por sus siglas en inglés) 504 antes de delinear la zona de protección 502. Además, o como una alternativa, el usuario 128 delinea la zona de protección 502 y después activa el modo SP 504. En un ejemplo particular, el modo SP 504 se activa al seleccionar un control de protección contra compartición ("proteger") 506. En general, el modo SP 504 permite que una porción de una pantalla se designe como protegida contra compartición. Por ejemplo, el modo SP 504 permite delinear una zona de protección alrededor de cualquier porción arbitraria del dispositivo de presentación 506, y el contenido dentro de la zona de protección se designará como protegido contra compartición.

Además del caso 500, delinear la zona de protección 502 hace que la porción del dispositivo de presentación 114 dentro de la zona de protección 502 se cifre utilizando una instancia de una clave 134. Los ejemplos de formas e implementaciones para cifrar el contenido protegido contra compartición se describieron anteriormente.

La figura 6 representa un caso de implementación 600 ejemplar para designar una región protegida contra compartición de acuerdo con una o más implementaciones. El caso 600 incluye varias entidades y componentes introducidos anteriormente con referencia al entorno 100. El caso 600, por ejemplo, puede implementarse junto con los casos 200-500 descritos anteriormente.

En el caso 600, el dispositivo cliente 102 está en el modo de compartición 216, tal como se describió anteriormente. Además, una GUI 602 incluye un control de protección 604. La GUI 602, por ejemplo, representa una GUI para una aplicación particular 108. De acuerdo con las implementaciones abordadas en el presente documento, el control de protección 604 es seleccionable para activar el modo SP 504 para la GUI 602. Por ejemplo, en respuesta al usuario 128 que selecciona el control de protección 604, se activa el modo SP 504 para la GUI 402. En consecuencia, el usuario 128 puede mover (por ejemplo, arrastrar) la GUI 602 dentro del dispositivo de presentación 114, y la GUI 602 seguirá estando protegida contra compartición. Por lo tanto, el modo SP 504 puede vincularse a una instancia particular de contenido (por

ejemplo, la GUI 402) de manera que el contenido se mantenga protegido en cualquier lugar donde se muestre el contenido.

En general, la activación del modo SP 504 para la GUI 602 provoca que la GUI 602 se cifre por el módulo de cifrado 130 utilizando una clave 134. Por lo tanto, cuando el escritorio 210 se comparte con otros dispositivos que no tienen acceso a la clave 134, el contenido de la GUI 602 no está accesible sin obstáculos, por ejemplo, el contenido está visualmente oculto. Sin embargo, otros dispositivos que tienen acceso a la clave 134 pueden descifrar y visualizar sin obstáculos el contenido de la GUI 602.

La figura 7 representa un caso de implementación 700 ejemplar para designar un conjunto de usuarios que tiene permitido visualizar una región protegida contra compartición de acuerdo con una o más implementaciones. El caso 700 incluye varias entidades y componentes introducidos anteriormente con referencia al entorno 100. El caso 700, por ejemplo, puede implementarse junto con los casos 200-600 descritos anteriormente.

En el caso 700, el usuario 128 participa en la sesión de comunicación 204 introducida anteriormente y el modo de compartición 216 está activo de tal manera que una porción del escritorio 210 se comparte con otros dispositivos que participan en la sesión de comunicación 204. Además, la región 218b se designa como protegida contra compartición, tal como se describió anteriormente. En respuesta a la designación de la región 218b como protegida contra compartición, el módulo de cifrado 130 cifra el contenido de la región 218b con una clave 134 para generar contenido de video cifrado 702.

Además del caso 700, se muestra una interfaz de cliente de comunicación 704 en el dispositivo de presentación 114. En general, la interfaz de cliente de comunicación 704 representa una interfaz para el cliente de comunicación 110 que permite al usuario 128 realizar diversas acciones y visualizar información diversa perteneciente a la sesión de comunicación 204. En este ejemplo particular, la interfaz de cliente de comunicación 704 incluye una región participante 706 que identifica a diferentes usuarios que están conectados y que participan en la sesión de comunicación 204. Por ejemplo, la región participante 706 está llena con iconos visuales que representan cada usuario diferente que está conectado a la sesión de comunicación 204.

Tal como se abordó anteriormente, al menos en algunas implementaciones, cuando un usuario designa una región particular de un área de presentación como protegida contra compartición, la región se cifra de tal manera que otros participantes en una experiencia de compartición de pantalla no puedan visualizar sin obstáculos el contenido de la región a menos que los participantes puedan descifrar el contenido. Por lo tanto, las implementaciones abordadas en el presente documento permiten a un usuario evitar que una región particular sea accesible para algunos usuarios, mientras permite que la región sea accesible para otros usuarios. El usuario 128, por ejemplo, puede identificar a ciertos usuarios a los cuales se les permite visualizar sin obstáculos el contenido en una región que se designó como protegida contra compartición.

Por ejemplo, en la interfaz de cliente de comunicación 704, un icono de usuario 708a y un icono de usuario 708b en la región de participante 704 tienen anotaciones visuales para indicar que los usuarios representados por los respectivos iconos 708a, 708b están designados como autorizados para visualizar

sin obstáculos el contenido protegido contra compartición. Los iconos 708a, 708b, por ejemplo, tienen como anotación la letra “S” para indicar que los usuarios respectivos están autorizados para la compartición.

En general, el usuario 128 puede designar a los usuarios como autorizados para la compartición de varias maneras. Por ejemplo, el usuario 202 puede seleccionar los iconos individuales 708a, 708b, como, clic en el botón derecho del mouse, gesto táctil de presionar y mantener presionado, gesto manual sin contacto, etcétera. En respuesta a la selección, al usuario 202 se le puede presentar una opción seleccionable que permite que los iconos 708a, 708b se designen como autorizados.

Además, o como una alternativa, el usuario 128 puede arrastrar los iconos 708a, 708b desde la región participante 706 a una región autorizada 708 de la interfaz de cliente de comunicaciones 702, lo cual hace que los usuarios respectivos se designen como autorizados para la compartición. La región autorizada 708, por ejemplo, está llena con iconos 708a, 708b para indicar que los usuarios respectivos están designados como autorizados para la compartición, de modo que los usuarios puedan obtener una clave de cifrado para descifrar el contenido protegido contra compartición.

Además del caso 700, en respuesta a los usuarios representados por los iconos 708a, 708b que se designan como autorizados para la compartición, una clave 710 se pone a disposición de los usuarios autorizados. De acuerdo con varias implementaciones, la clave 710 representa una instancia (por ejemplo, una copia) de la clave 134 que se utilizó para cifrar el contenido cifrado 702. La clave 710, por ejemplo, puede comunicarse a los usuarios autorizados, como a través de correo electrónico, mensajería de Internet, mensajería de texto, etcétera. Además, o como una alternativa, la clave 710 puede comunicarse directamente a las respectivas instancias de los clientes de comunicación 118 que residen en los dispositivos terminales 116 asociados con los usuarios autorizados. Como otra implementación más, la clave 710 puede almacenarse en una ubicación remota a la cual pueden acceder los usuarios autorizados, como un almacenamiento de red que está remoto a los dispositivos terminales 116 asociados con los usuarios respectivos.

Tal como se mencionó anteriormente, el acceso a una clave para descifrar contenido protegido contra compartición puede basarse en la membresía a un grupo. Por lo tanto, en al menos algunas implementaciones, la clave 710 puede compartirse con los usuarios autorizados al asociar la clave 710 con un grupo particular. Por ejemplo, en respuesta a los usuarios designados como usuarios autorizados, los usuarios pueden agregarse como miembros de un grupo 712 que tiene acceso a la clave 710. Por lo tanto, los dispositivos terminales 118 asociados con los usuarios autorizados pueden acceder a la clave 710, como al acceder a un almacenamiento de red que almacena el contenido para el grupo 712. Alternativamente, los usuarios autorizados pueden ya ser miembros del grupo 712 y, por lo tanto, el grupo 712 puede designarse como un grupo autorizado en respuesta a los usuarios designados como autorizados. Así, debido a que al ser miembros del grupo 712, los usuarios autorizados representados por los iconos 706a, 706b pueden acceder a la clave 710 y descifrar el contenido cifrado 702 para permitir que los usuarios autorizados visualicen sin obstáculos el contenido en la región 218b.

Si el usuario 128 desea rescindir la autorización de compartición para un usuario particular, el usuario 128 puede realizar una acción para hacerlo. Por ejemplo, el usuario 128 puede seleccionar un

ícono individual 706a, 706b y se le presentará una opción para suspender el permiso de compartición para el usuario respectivo. Si el usuario 128 selecciona la opción, el permiso de compartición para el usuario se rescindirá de tal manera que el contenido designado como autorizado para compartición ya no será accesible para el usuario. Además, o como una alternativa, el usuario 128 puede arrastrar un ícono 706a, 706b desde la región autorizada 708 a la región participante 704, lo cual hace que el permiso de compartición para el usuario respectivo se desactive. En general, la rescisión del permiso de compartición puede ocurrir de varias maneras. Por ejemplo, el acceso a la clave 710 puede rescindirse de manera que el usuario ya no pueda acceder a la clave 710 y descifrar el contenido cifrado 702.

Alternativamente, puede seleccionarse una clave 134 diferente para cifrar el contenido protegido contra compartición para generar el contenido 702 cifrado, de modo que la clave 710 ya no sea efectiva para descifrar el contenido 702 cifrado. En tal caso, puede distribuirse la clave diferente y/o se pone a disposición de otros usuarios que aún están autorizados para la compartición, pero no para el usuario a que se le rescindió el permiso de compartición.

En al menos algunas implementaciones, los usuarios pueden designarse como autorizados y no autorizados dinámicamente, como cuando la sesión de comunicación 204 está en progreso. Por ejemplo, cabe destacar que el usuario ha designado a la región 218b como protegida contra compartición, tal como se describió anteriormente. Además, mientras la sesión de comunicación 204 está en progreso, el usuario 128 desea compartir temporalmente la región 218b con un subconjunto de participantes en la sesión de comunicación 204. En consecuencia, mientras la sesión de comunicación 204 está en progreso, el usuario puede realizar una acción para designar los usuarios representados por los íconos 706a, 706b como autorizados para la compartición. En respuesta, la región 218b pasará de estar protegida contra compartición para los usuarios, a compartirse con los usuarios de tal manera que los usuarios puedan visualizar sin obstáculos la región 218b en sus dispositivos respectivos mientras la región 218b permanece protegida para otros usuarios no autorizados que participan en la sesión de comunicación. Si el usuario 128 decide posteriormente, mientras la sesión de comunicación 204 está en progreso, proteger contra compartición la región 218b para los usuarios, el usuario 128 puede rescindir el permiso de compartición de los usuarios, tal como se describió anteriormente. Por lo tanto, las implementaciones para la protección contra compartición para una experiencia de compartición de pantalla permiten que las regiones protegidas contra compartición se compartan temporalmente con diferentes usuarios mientras una sesión de comunicación está en progreso.

La figura 8 muestra un caso de implementación 800 ejemplar para designar usuarios que están autorizados para la compartición de acuerdo con una o más implementaciones. El caso 800 incluye varias entidades y componentes introducidos anteriormente con referencia al entorno 100. El caso 800, por ejemplo, puede implementarse junto con los casos 200-700 descritos anteriormente.

El caso 800 incluye una GUI de invitación a la reunión (“GUI de invitación”) 802, que representa una GUI para generar una invitación para que diferentes usuarios participen en una sesión de comunicación 804 implementada a través del cliente de comunicación 110. La sesión de comunicación 804, por ejemplo, representa una sesión de comunicación que se producirá en un momento futuro. La GUI de invitación 802

incluye una región de invitados 806 y una región de autorizados para compartición 808. En general, la región de invitados 806 permite al usuario 128 especificar diferentes usuarios que serán invitados a participar en una sesión de comunicación. La región de autorizados para compartición 808 permite al usuario 128 indicar si los usuarios particulares identificados en la región de invitados están autorizados para la compartición. En este ejemplo particular, la región de autorizados para compartición 808 incluye controles seleccionables que permiten que el estado de autorización de compartición para los usuarios individuales pueda seleccionarse y deseleccionarse. Por ejemplo, en este caso, los usuarios “A Smith” y “W Sole” están designados como autorizados para la compartición, mientras los usuarios “T Heins” y “J Owen” no lo están.

La GUI de invitación 802 incluye un control de envío 810, que puede seleccionarse para provocar que las invitaciones 812 para participar en la sesión de comunicación 804 se envíen a los invitados identificados en la región de invitados 804. En general, las invitaciones 810 pueden enviarse en varias formas, como correo electrónico, mensajería por internet, comunicación entre aplicaciones (por ejemplo, entre diferentes instancias de los clientes de comunicación 110), etcétera.

En general, las invitaciones 810 incluyen invitaciones estándar 814 e invitaciones de autorización 816. Las invitaciones estándar 814 se envían a invitados que no están designados como autorizados para compartición, por ejemplo, “T Heins” y “J Owen”. Sin embargo, las invitaciones de autorización 816 se envían a invitados designados como autorizados, por ejemplo, “A Smith” y “W Sole”. Las invitaciones de autorización 816, por ejemplo, brindan acceso a una clave 818 que puede utilizarse para descifrar contenido que se designa como protegido contra compartición como parte de la sesión de comunicación 804. La clave 818, por ejemplo, puede adjuntarse a las invitaciones de autorización 816, pero no a las invitaciones estándar 812. Además, o como una alternativa, las invitaciones de autorización 816 pueden incluir un enlace (por ejemplo, un hipervínculo) u otro enlace a una ubicación de red donde puede recuperarse la clave 818, como una ubicación de almacenamiento de red segura. Por ejemplo, una invitación de autorización 816 puede incluir un enlace a la clave 818 sin incluir la clave 818 en sí. En otro ejemplo de implementación, el envío de las invitaciones de autorización 816 provoca que los usuarios autorizados para la compartición se agreguen a un grupo autorizado al cual se le permite acceder a la clave 818.

En contraste, las invitaciones estándar 814 no proporcionan acceso a la clave 818 y, por lo tanto, no permiten que los invitados no autorizados para la compartición accedan a la clave y descifren contenido protegido contra compartición incluido como parte de la sesión de comunicación 804. En un caso donde se emplea el acceso grupal, las invitaciones estándar 814 no provocan que los usuarios no autorizados para la compartición se agreguen al grupo autorizado para la compartición.

Por lo tanto, estos casos ejemplares demuestran que las técnicas de protección contra compartición para una experiencia de compartición de pantalla permiten compartir el contenido de la pantalla que estará protegido contra compartición como parte de una experiencia de compartición de pantalla, y permiten que ciertos participantes en la experiencia de compartición de pantalla visualicen sin obstáculos el contenido protegido contra compartición.

Tras abordar algunos casos de implementación ejemplares, ahora se considera un análisis de

algunos procedimientos ejemplares de acuerdo con una o más modalidades.

El siguiente análisis describe algunos procedimientos ejemplares de la protección contra compartición para una experiencia de compartición de pantalla de acuerdo con una o más modalidades. Los procedimientos ejemplares pueden emplearse en el entorno 100 de la figura 1, el sistema 1200 de la figura 12, y/o cualquier otro entorno adecuado. Los procedimientos, por ejemplo, representan los procedimientos ejemplares para implementar los casos de implementación descritos anteriormente. En al menos algunas implementaciones, las etapas descritas para los diversos procedimientos se implementan de forma automática e independiente de la interacción del usuario. De acuerdo con diversas implementaciones, los procedimientos pueden realizarse localmente (por ejemplo, en el dispositivo cliente 102) y/o en un servicio basado en la red, como el servicio de comunicación 120.

La figura 9 es un diagrama de flujo que describe las etapas de un método de acuerdo con una o más implementaciones. El método describe un procedimiento ejemplar para controlar el acceso al contenido de una región protegida contra compartición de acuerdo con una o más implementaciones. En al menos algunas implementaciones, el método puede realizarse al menos en parte en el dispositivo cliente 102 (por ejemplo, mediante el cliente de comunicaciones 110) y/o mediante el servicio de comunicaciones 120.

La etapa 900 determina que una región de medios compartidos debe protegerse contra compartición como parte de una experiencia de compartición de pantalla. Un usuario, por ejemplo, selecciona una región particular de un área de presentación y/o un tipo de contenido particular que se protegerá contra compartición. Pueden emplearse de manera adicional o alternativa otras formas de seleccionar contenido protegido contra compartición, como a través de la selección de contenido en un entorno de realidad virtual/combinada, selección de contenido presentado en un dispositivo de presentación remoto, etcétera. Los ejemplos de formas de designar una región de presentación y/o contenido particular (por ejemplo, “medios compartidos”) como protegidos contra compartición se abordaron anteriormente.

La etapa 902 recibe la entrada del usuario que especifica un primer participante en la experiencia de compartición de pantalla que debe tener acceso al contenido de la región de los medios compartidos. Las diferentes formas de especificar un usuario autorizado para la compartición se describieron anteriormente.

La etapa 904 provoca que el contenido de la región se cifre con una clave durante la experiencia de compartición de pantalla entre un grupo de participantes en la experiencia de compartición de pantalla. El módulo de cifrado 130, por ejemplo, cifra el contenido con una clave de cifrado 134 para generar el contenido cifrado.

La etapa 906 designa a un primer participante del grupo de participantes como autorizado para la compartición para acceder a la clave y no designa a un segundo participante del grupo de participantes como autorizado para la compartición para acceder a la clave. En general, esto permite que la clave sea accesible para el primer participante para que el contenido se descifre para el primer participante como parte de la experiencia de compartición de pantalla, pero no permite que la clave sea accesible para el

segundo participante como parte de la experiencia de compartición de pantalla. Por ejemplo, a un primer dispositivo asociado con el primer participante se le permite el acceso a la clave para permitir que el primer dispositivo descifre el contenido como parte de la experiencia de compartición de pantalla, pero un segundo dispositivo asociado con el segundo participante no tiene permitido el acceso a la clave como parte de la experiencia de compartición de pantalla.

La etapa 908 comunica el contenido cifrado junto con otro contenido no cifrado como parte de un flujo de datos de la experiencia de compartición de pantalla. En al menos algunas implementaciones, la experiencia de compartición de pantalla es parte de una sesión de comunicación en tiempo real. Por lo tanto, las porciones de una región de presentación pueden cifrarse e incluirse en el flujo de datos, mientras otras porciones pueden incluirse en el flujo de datos en una forma no cifrada.

La figura 10 es un diagrama de flujo que describe las etapas de un método de acuerdo con una o más implementaciones. El método describe un procedimiento ejemplar para controlar el acceso al contenido de una región protegida contra compartición de acuerdo con una o más implementaciones. En al menos algunas implementaciones, el método puede realizarse al menos en parte en el dispositivo cliente 102 (por ejemplo, mediante el cliente de comunicaciones 110) y/o mediante el servicio de comunicaciones 120.

La etapa 1000 envía una invitación de autorización para una sesión de comunicación a un primer participante, la invitación de autorización permite el acceso a una clave que se utiliza para cifrar contenido protegido. El cliente de comunicación 110, por ejemplo, comunica una invitación de autorización a un usuario que se designa como autorizado para la compartición. De acuerdo con varias implementaciones, la invitación de autorización permite el acceso a una clave de cifrado para cifrar el contenido protegido cifrado. Por ejemplo, un primer dispositivo asociado con el primer participante puede utilizar la información asociada con la invitación para acceder a la clave y descifrar el contenido cifrado.

La etapa 1002 envía una invitación estándar para la sesión de comunicación a un segundo participante, la invitación estándar no permite el acceso a la clave. La invitación estándar, por ejemplo, permite al primer participante participar en la sesión de comunicación, pero no descifrar el contenido protegido que se transmite en forma cifrada como parte de la sesión de comunicación.

En general, los procedimientos mencionados anteriormente pueden realizarse dinámicamente y en tiempo real mientras está activa una experiencia de compartición de pantalla (por ejemplo, una sesión de comunicación). Por ejemplo, mientras la experiencia de compartición de pantalla está activa, un usuario compartidor puede designar a un usuario como autorizado para la compartición, de modo que el dispositivo de otro usuario pueda acceder a una clave de cifrado para descifrar el contenido protegido. Además, mientras la experiencia de compartición de pantalla aún está activa, el usuario compartidor puede revocar el estado de autorización de compartición del usuario, de modo que se revoque el permiso del usuario para acceder a una clave de cifrado para descifrar el contenido.

La figura 11 es un diagrama de flujo que describe las etapas de un método de acuerdo con una o más implementaciones. El método describe un procedimiento ejemplar para ocultar visualmente una región protegida contra compartición de acuerdo con una o más implementaciones. En al menos algunas

implementaciones, el método puede realizarse al menos en parte en el dispositivo cliente 102 (por ejemplo, mediante el cliente de comunicaciones 110) y/o mediante el servicio de comunicaciones 120.

La etapa 1100 determina que una primera región de un área de presentación de un dispositivo cliente se protegerá contra compartición. Un usuario, por ejemplo, proporciona información para identificar una porción de un área de presentación que se protegerá contra compartición.

La etapa 1102 provoca que la primera región se cifre en el dispositivo cliente de modo que la primera región esté visualmente oculta en el área de presentación del dispositivo cliente. Por ejemplo, en respuesta a la determinación de que la primera región del área de presentación se protegerá contra compartición, el contenido de la primera región está cifrado.

La etapa 1104 captura una imagen de video del área de presentación que incluye la primera región oculta visualmente y una segunda región no oculta del área de presentación del dispositivo cliente. Una región diferente del área de presentación, por ejemplo, no está designada como protegida contra compartición y, por lo tanto, no está cifrada. Por consiguiente, la primera región cifrada y la segunda región no cifrada pueden capturarse juntas como una única imagen de video de un área de presentación. De acuerdo con varias implementaciones, la imagen de video única representa una imagen en tiempo real que se captura durante un período de tiempo, como parte de una sesión de comunicación en tiempo real.

La etapa 1106 comunica la imagen de video a un dispositivo diferente como parte de una experiencia de compartición de pantalla entre el dispositivo cliente y el dispositivo diferente. Por ejemplo, la imagen de video se comunica como parte de un flujo de datos entre el dispositivo cliente y el dispositivo diferente, como parte de una sesión de comunicación en tiempo real entre los dispositivos.

De acuerdo con las implementaciones abordadas en el presente documento, los procedimientos descritos anteriormente pueden realizarse varias veces durante una sesión de comunicación para designar las regiones protegidas contra compartición de un área de presentación, y para identificar a los usuarios que está autorizados para la compartición.

Por consiguiente, las técnicas abordadas en el presente documento proporcionan una amplia variedad de casos e implementaciones para permitir que se comparta parte de contenido durante una experiencia de compartición de pantalla, mientras se protege el acceso sin obstáculos a otro contenido durante la experiencia. Esto mejora la capacidad de un usuario para compartir cierto contenido durante una experiencia de compartición de pantalla, mientras protege otro contenido confidencial durante la experiencia.

Tras abordar algunos procedimientos ejemplares, ahora se considera un análisis de un sistema y dispositivo ejemplares de acuerdo con una o más modalidades.

La figura 12 ilustra un sistema ejemplar generalmente con el número de referencia 1200 que incluye un dispositivo informático 1202 ejemplar que es representativo de uno o más sistemas y/o dispositivos informáticos que pueden implementar diversas técnicas descritas en el presente documento. Por ejemplo, el dispositivo cliente 102, dispositivos terminales 116 y/o servicio de comunicación 120 abordados anteriormente con referencia a la figura 1, pueden incorporarse como el dispositivo informático 1202. El dispositivo informático 1202 puede ser, por ejemplo, un servidor de un proveedor de servicios, un

dispositivo asociado con el cliente (por ejemplo, un dispositivo cliente), un sistema en chip y/o cualquier otro dispositivo informático o sistema informático adecuado.

El dispositivo informático 1202 ejemplar, tal como se ilustra, incluye un sistema de procesamiento 1204, uno o más medios legibles por computadora 1206, y una o más interfaces de entrada/salida (I/O, por sus siglas en inglés) 1208 que están conectados comunicativamente entre sí. Aunque no se muestra, el dispositivo informático 1202 puede incluir además un bus de sistema u otro sistema de transferencia de datos y comandos que conecta los diversos componentes entre sí. Un bus de sistema puede incluir cualquiera o una combinación de diferentes estructuras de bus, como un bus de memoria o un controlador de memoria, bus de periféricos, bus serial universal y/o un procesador o bus local que utilice cualquiera de una variedad de arquitecturas de bus. También se contempla una variedad de otros ejemplos, como las líneas de control y de datos.

El sistema de procesamiento 1204 es representativo de la funcionalidad para realizar una o más operaciones utilizando *hardware*. Por consiguiente, se ilustra que el sistema de procesamiento 1204 incluye un elemento de *hardware* 1210 que puede configurarse como procesadores, bloques funcionales, etcétera. Esto puede incluir la implementación en *hardware* como un circuito integrado de aplicación específica u otro dispositivo lógico formado utilizando uno o más semiconductores. Los elementos de *hardware* 1210 no están limitados por los materiales a partir de los cuales se fabrican o mecanismos de procesamiento empleados en los mismos. Por ejemplo, los procesadores pueden estar compuestos por semiconductores y/o transistores (por ejemplo, circuitos integrados (IC, por sus siglas en inglés) electrónicos). En este contexto, las instrucciones ejecutables por el procesador pueden ser instrucciones electrónicamente ejecutables.

Se ilustra que el medio legible por computadora 1206 incluye la memoria/almacenamiento 1212. La memoria/almacenamiento 1212 representa la capacidad de memoria/almacenamiento asociada con uno o más medios legibles por computadora. La memoria/almacenamiento 1212 puede incluir medios volátiles (como memoria de acceso aleatorio (RAM, por sus siglas en inglés)) y/o medios no volátiles (como memoria exclusivamente de lectura (ROM, por sus siglas en inglés), memoria *flash*, discos ópticos, discos magnéticos, etcétera). La memoria/almacenamiento 1212 puede incluir medios fijos (por ejemplo, RAM, ROM, disco duro fijo, etcétera) así como medios extraíbles (por ejemplo, memoria *flash*, disco duro extraíble, disco óptico, etcétera). El medio legible por computadora 1206 puede configurarse de una variedad de otras formas tal como se describirá posteriormente.

Las interfaces de entrada/salida 1208 son representativas de la funcionalidad para permitir que un usuario ingrese comandos e información al dispositivo informático 1202, y también permite que la información se presente al usuario y/o a otros componentes o dispositivos que utilizan varias entradas/dispositivos de salida. Los ejemplos de dispositivos de entrada incluyen un teclado, un dispositivo de control de cursor (por ejemplo, un ratón), un micrófono (por ejemplo, para reconocimiento de voz y/o entrada hablada), un escáner, funcionalidad táctil (por ejemplo, sensores capacitivos u otros sensores que están configurados para detectar el contacto físico), una cámara (por ejemplo, que puede emplear longitudes de onda visibles o no visibles, como las frecuencias infrarrojas para detectar movimientos que

no impliquen contacto como gestos), etcétera. Los ejemplos de dispositivos de salida incluyen un dispositivo de presentación (por ejemplo, un monitor o proyector), altavoces, una impresora, una tarjeta de red, un dispositivo de respuesta táctil, etcétera. Por lo tanto, el dispositivo informático 1202 puede configurarse de varias maneras, tal como se describirá con más detalle posteriormente, para ser compatible con la interacción del usuario.

Pueden describirse varias técnicas en el presente documento en el contexto general del *software*, elementos de *hardware* o módulos de programas. En general, tales módulos incluyen rutinas, programas, objetos, elementos, componentes, estructuras de datos, etcétera, que realizan tareas particulares o implementan tipos de datos abstractos particulares. Los términos “módulo”, “funcionalidad”, “entidad” y “componente” tal como se utilizan en el presente documento generalmente representan *software*, *firmware*, *hardware* o una combinación de los mismos. Las características de las técnicas descritas en el presente documento son independientes de la plataforma, lo cual significa que las técnicas pueden implementarse en una variedad de plataformas de informática comerciales que tienen una variedad de procesadores.

Una implementación de los módulos y técnicas descritas puede almacenarse o transmitirse a través de algún tipo de medio legible por computadora. Los medios legibles por computadora pueden incluir una variedad de medios a los cuales puede acceder el dispositivo informático 1202. A modo de ejemplo, y no como limitación, los medios legibles por computadora pueden incluir “medios de almacenamiento legibles por computadora” y “medios de señal legibles por computadora”.

Los “medios de almacenamiento legibles por computadora” pueden referirse a medios y/o dispositivos que permiten el almacenamiento persistente de información en contraste con la mera transmisión de señales, ondas portadoras o señales *per se*. Los medios de almacenamiento legibles por computadora no incluyen señales *per se*. Los medios de almacenamiento legibles por computadora incluyen *hardware* como dispositivos volátiles y no volátiles, extraíbles y no extraíbles y/o dispositivos de almacenamiento implementados en un método o tecnología adecuada para el almacenamiento de información como instrucciones legibles por computadora, estructuras de datos, módulos de programas, elementos lógicos/circuitos, u otros datos. Los ejemplos de medios de almacenamiento legibles por computadora pueden incluir, entre otros, RAM, ROM, EEPROM, memoria *flash* u otra tecnología de memoria, CD-ROM, discos versátiles digitales (DVD, por sus siglas en inglés) u otro almacenamiento óptico, discos duros, casetes magnéticos, cinta magnética, almacenamiento en disco magnético u otros dispositivos de almacenamiento magnético, u otro dispositivo de almacenamiento, medio tangible o artículo de fabricación adecuado para almacenar la información deseada y al que puede accederse desde una computadora.

El “medio de señal legible por computadora” puede referirse a un medio portador de señal que está configurado para transmitir instrucciones al *hardware* del dispositivo informático 1202, por ejemplo, a través de una red. Los medios de señal generalmente pueden incluir instrucciones legibles por computadora, estructuras de datos, módulos de programa u otros datos en una señal de datos modulada, como ondas portadoras, señales de datos u otros mecanismos de transporte. Los medios de señal también incluyen cualquier medio de suministro de información. El término “señal de datos modulada” significa una señal

que tiene una o más de sus características configuradas o modificadas de tal manera que codifiquen la información en la señal. A modo de ejemplo, y no de limitación, los medios de comunicación incluyen medios alámbricos, como una red alámbrica o conexión directa, y medios inalámbricos, como acústicos, radiofrecuencia (RF, por sus siglas en inglés), infrarrojos y otros medios inalámbricos.

5 Tal como se describió anteriormente, los elementos de *hardware* 1210 y los medios legibles por computadora 1206 son representativos de instrucciones, módulos, lógica de dispositivo programable y/o lógica de dispositivo fijo implementados en una forma de *hardware* que puede emplearse en algunas modalidades para implementar al menos algunos aspectos de las técnicas descritas en el presente documento. Los elementos de *hardware* pueden incluir componentes de un circuito integrado o sistema en
10 chip, circuito integrado de aplicación específica (ASIC, por sus siglas en inglés), matriz de puertas programable *in-situ* (FPGA, por sus siglas en inglés), dispositivo complejo de lógica programable (CPLD, por sus siglas en inglés) y otras implementaciones en silicio u otros dispositivos de *hardware*. En este contexto, un elemento de *hardware* puede operar como un dispositivo de procesamiento que realiza las tareas de programa definidas por instrucciones, módulos, y/o lógica incorporados por el elemento de
15 *hardware*, así como un dispositivo de *hardware* utilizado para almacenar las instrucciones para la ejecución, por ejemplo, los medios de almacenamiento legibles por computadora descritos previamente.

Las combinaciones de los anteriores también pueden emplearse para aplicar diversas técnicas y módulos descritos en el presente documento. De acuerdo con ello, los módulos de *software*, *hardware* o programa y otros módulos de programa, pueden implementarse como una o más instrucciones y/o lógica
20 incorporadas en alguna forma de medios de almacenamiento legibles por computadora y/o por uno o más elementos de *hardware* 1210. El dispositivo informático 1202 puede configurarse para implementar instrucciones y/o funciones particulares correspondientes a los módulos de *hardware* y/o *software*. En consecuencia, la implementación de los módulos que son ejecutables por el dispositivo informático 1202 como *software* puede obtenerse al menos parcialmente en *hardware*, por ejemplo, a través del uso de
25 medios de almacenamiento legibles por computadora y/o elementos de *hardware* 1210 del sistema de procesamiento. Las instrucciones y/o funciones pueden ejecutarse/operarse por uno o más artículos de fabricación (por ejemplo, uno o más dispositivos informáticos 1202 y/o sistemas de procesamiento 1204) para implementar las técnicas, módulos, y ejemplos descritos en el presente documento.

Tal como se ilustra, además, en la figura 12, el sistema ejemplar 1200 permite los entornos ubicuos
30 para una experiencia de usuario ininterrumpida cuando se ejecutan las aplicaciones en una computadora personal (PC, por sus siglas en inglés), un dispositivo de televisión, y/o un dispositivo móvil. Los servicios y aplicaciones se ejecutan sustancialmente de manera similar en los tres entornos para una experiencia de usuario común al realizar la transición de un dispositivo al próximo dispositivo utilizando una aplicación, jugar un videojuego, ver un video, etcétera.

35 En el sistema ejemplar 1200, múltiples dispositivos están interconectados a través de un dispositivo informático central. El dispositivo informático central puede estar en el mismo lugar que los múltiples dispositivos o puede ubicarse a distancia de los múltiples dispositivos. En una modalidad, el dispositivo informático central puede ser una nube de una o más computadoras servidor que se conecta a los múltiples

dispositivos a través de una red, internet, u otro enlace de comunicación de datos.

En una modalidad, esta arquitectura de interconexión activa la funcionalidad que se suministrará a través de múltiples dispositivos para proporcionar una experiencia común e ininterrumpida a un usuario de los múltiples dispositivos. Cada uno de los múltiples dispositivos puede tener diferentes requisitos físicos y capacidades, y el dispositivo informático central utiliza una plataforma para permitir el suministro de una experiencia al dispositivo que esté a la vez adaptada al dispositivo y, sin embargo, sea común para todos los dispositivos. En una modalidad, se crea una clase de dispositivos específicos y las experiencias se adaptan a la clase genérica de dispositivos. Una clase de dispositivos puede definirse por las características físicas, tipos de uso u otras características comunes de los dispositivos.

En diversas implementaciones, el dispositivo informático 702 puede asumir una variedad de diferentes configuraciones, como para usos en computadora 1214, móvil 1216, y televisión 1218. Cada una de estas configuraciones incluye dispositivos que pueden tener en general diferentes construcciones y capacidades, y, por lo tanto, el dispositivo informático 1202 puede configurarse de acuerdo con una o más de las diferentes clases de dispositivos. Por ejemplo, el dispositivo informático 1202 puede implementarse como la clase computadora 1214 de un dispositivo que incluye una computadora personal, computadora de sobremesa, computadora de múltiples pantallas, computadora portátil, minicomputadora portátil, etcétera.

El dispositivo informático 1202 también puede implementarse como clase móvil 1216 de dispositivos que incluye los dispositivos móviles, como un teléfono móvil, reproductor de música portátil, dispositivo de juegos portátil, computadora tipo tableta, computadora de múltiples pantallas, etcétera. El dispositivo informático 1202 también puede implementarse como la clase televisión 1218 de dispositivos que incluye los dispositivos que tienen o están conectados a pantallas generalmente más grandes en entornos casuales de visualización. Estos dispositivos incluyen televisores, convertidores de señal de TV, consolas de juegos, etcétera.

Las técnicas descritas en el presente documento pueden ser compatibles con estas diversas configuraciones del dispositivo informático 1202 y no se limitan a los ejemplos específicos de las técnicas descritas en el presente documento. Por ejemplo, las funcionalidades abordadas con referencia al módulo de compartición 122, módulo de cifrado 130 y/o servicio de comunicación 120 pueden implementarse completamente o en parte a través del uso de un sistema distribuido, como, por ejemplo, en una “nube” 1220 a través de una plataforma 1222, tal como se describe a continuación.

La nube 1220 incluye y/o es representativa de una plataforma 1222 de recursos 1224. La plataforma 1222 extrae la funcionalidad subyacente del *hardware* (por ejemplo, servidores) y los recursos de *software* de la nube 1220. Los recursos 1224 pueden incluir aplicaciones y/o datos que pueden utilizarse mientras el procesamiento informático se ejecuta en los servidores que se encuentran a distancia del dispositivo informático 1202. Los recursos 1224 también pueden incluir los servicios prestados a través de internet y/o a través de una red de suscriptor, como una red celular o *wifi*.

La plataforma 1222 puede extraer los recursos y funciones para conectar el dispositivo informático 1202 con otros dispositivos informáticos. La plataforma 1222 puede servir también para extraer el ajuste

de la escala de recursos para proporcionar un nivel correspondiente de escala a la demanda encontrada por los recursos 1224 que se implementan a través de la plataforma 1222. En consecuencia, en una modalidad del dispositivo interconectado, la implementación de la funcionalidad descrita en el presente documento puede distribuirse en todo el sistema 1200. Por ejemplo, la funcionalidad puede implementarse en parte en el dispositivo informático 1202, así como a través de la plataforma 1222 que extrae la funcionalidad de la nube 1220.

En el presente documento se abordan varios métodos que pueden implementarse para realizar las técnicas abordadas en el presente documento. Los aspectos de los métodos pueden implementarse en *hardware*, *firmware* o *software*, o una combinación de los mismos. Los métodos se muestran como un conjunto de etapas que especifican las operaciones realizadas por uno o más dispositivos y no están necesariamente limitados a las órdenes mostradas para realizar las operaciones por los bloques respectivos. Además, una operación mostrada con respecto a un método particular puede combinarse y/o intercambiarse con una operación de un método diferente de acuerdo con una o más implementaciones. Los aspectos de los métodos pueden implementarse a través de la interacción entre varias entidades abordadas anteriormente con referencia al entorno 1200.

Se describen las técnicas de protección contra compartición para una experiencia de compartición de pantalla. Aunque las modalidades se describen en un lenguaje específico para características estructurales y/o acciones metodológicas, debe entenderse que las modalidades definidas en las reivindicaciones adjuntas no están necesariamente limitadas a las características o acciones específicas descritas. Más bien, las características y acciones específicas se describen como formas de implementación ejemplares de las modalidades reivindicadas.

En los análisis en el presente documento, se describen varias modalidades diferentes. Debe apreciarse y entenderse que cada modalidad descrita en el presente documento puede utilizarse por sí sola o con relación a una o más modalidades descritas en el presente documento. Otros aspectos de las técnicas abordadas en el presente documento se relacionan con una o más de las siguientes modalidades:

Un sistema para proteger medios para una experiencia de compartición de pantalla, el sistema comprende: al menos un procesador; y uno o más medios de almacenamiento legibles por computadora, que incluyen las instrucciones almacenadas en los mismos que, en respuesta a la ejecución por al menos un procesador, provocan que el sistema realice las operaciones que incluyen: verificar que una región de medios compartidos se protegerá contra compartición como parte de una experiencia de compartición de pantalla; provocar que el contenido de la región se cifre con una clave durante la experiencia de compartición de pantalla entre un grupo de participantes en la experiencia de compartición de pantalla; y designar a un primer participante del grupo de participantes como autorizado para la compartición, de modo que se permita que la clave sea accesible para el primer participante para permitir que el contenido se descifre para el primer participante como parte de la experiencia de compartición de pantalla, y un segundo participante del grupo de participantes no está designado como autorizado para la compartición, por lo cual no se permite que la clave sea accesible para el segundo participante como parte de la experiencia de compartición de pantalla.

Además de cualquiera de los sistemas descritos anteriormente, cualquiera o combinación de: donde dicha determinación responde a la entrada del usuario que identifica la región de los medios compartidos; donde la región de medios compartidos corresponde a una región de un área de presentación de un dispositivo cliente; donde dicha designación permite que la clave sea accesible para un primer dispositivo asociado con el primer participante, pero no permite que la clave sea accesible para un segundo dispositivo asociado con el segundo participante; donde la experiencia de compartición de pantalla comprende una sesión de comunicación, y donde dicha designación del primer participante como autorizado para la compartición se basa en la entrada del usuario que especifica que el primer participante es un usuario autorizado, la entrada del usuario comprende la interacción del usuario con una invitación a la reunión para la sesión de comunicación; donde la experiencia de compartición de pantalla comprende una sesión de comunicación, y donde dicha designación del primer participante como autorizado para la compartición provoca que la clave se adjunte a una invitación a la reunión para la sesión de comunicación que se envía al primer participante; donde la experiencia de compartición de pantalla comprende una sesión de comunicación, y donde dicha designación del primer participante como autorizado para la compartición produce un enlace a la clave incluido con una invitación a la reunión para la sesión de comunicación que se envía al primer participante; donde dicha designación del primer participante como autorizado para la compartición se basa en una membresía a un grupo del primer participante, y donde la clave es accesible para los miembros del grupo; donde la experiencia de compartición de pantalla comprende una sesión de comunicación, y donde las operaciones incluyen, además: enviar una invitación de autorización para la sesión de comunicación al primer participante, la invitación de autorización permite el acceso a la clave; y enviar una invitación estándar para la sesión de comunicación al segundo participante, la invitación estándar no permite el acceso a la clave; donde las operaciones incluyen además provocar que un flujo de datos se comunique a un primer dispositivo asociado con el primer participante y un segundo dispositivo asociado con el segundo participante como parte de la experiencia de compartición de pantalla, el flujo de datos incluye contenido cifrado de la región junto con diferente contenido de una región diferente de los medios compartidos que no está cifrado con la clave; donde la región de medios compartidos corresponde a una región de un dispositivo de presentación de un dispositivo cliente, la experiencia de compartición de pantalla comprende una sesión de comunicación en tiempo real que incluye el dispositivo cliente, un primer dispositivo asociado con el primer participante, y un segundo dispositivo asociado con el segundo participante, y donde dicha provocación y designación se realizan dinámicamente durante la sesión de comunicación.

Un método implementado por computadora para proteger los medios para una experiencia de compartición de pantalla, que comprende: determinar que una primera región de un área de presentación de un dispositivo cliente debe protegerse contra compartición; provocar, en respuesta a dicha comprobación, que la primera región se cifre en el dispositivo cliente de manera que la primera región esté visualmente oculta en el área de presentación del dispositivo cliente; capturar una imagen de video del área de presentación que incluye la primera región visualmente oculta y una segunda región no oculta del área de presentación del dispositivo cliente; y comunicar la imagen de video a un dispositivo diferente como

parte de una experiencia de compartición de pantalla entre el dispositivo cliente y el dispositivo diferente.

Además de cualquiera de los métodos descritos anteriormente, cualquiera o combinación de: comprende, además, codificar la imagen de video como un único flujo de datos codificados, y donde dicha comunicación comprende comunicar el único flujo de video codificado al dispositivo diferente para permitir una representación visual de la primera región oculta y segunda región no oculta que se presentará en el dispositivo diferente; donde la experiencia de compartición de pantalla comprende una sesión de comunicación en tiempo real que incluye el dispositivo cliente y el dispositivo diferente; donde dicha determinación se basa en la entrada del usuario que identifica la primera región como protegida contra compartición.

Un método implementado por computadora para proteger los medios para una experiencia de compartición de pantalla, que comprende: determinar que una región de medios compartidos debe protegerse contra compartición como parte de una experiencia de compartición de pantalla; recibir la entrada del usuario que especifica un primer participante en la experiencia de compartición de pantalla que debe tener acceso al contenido de la región de los medios compartidos; hacer que el contenido de la región se cifre con una clave durante la experiencia de compartición de pantalla entre un grupo de participantes en la experiencia de compartición de pantalla; y designar al primer participante del grupo de participantes como autorizado para la compartición, de modo que se permita que la clave sea accesible para el primer participante para permitir que el contenido sea descifrado para el primer participante como parte de la experiencia de compartición de pantalla, y un segundo participante del grupo de participantes no está designado como autorizado para la compartición, por lo cual no se permite que la clave sea accesible para el segundo participante como parte de la experiencia de compartición de pantalla.

Además de cualquiera de los métodos descritos anteriormente, cualquiera o combinación de: donde la experiencia de compartición de pantalla comprende una sesión de comunicación, y donde dicha designación del primer participante como autorizado para la compartición provoca que la clave se adjunte a una invitación a una reunión para la sesión de comunicación que se envía al primer participante; donde la experiencia de compartición de pantalla comprende una sesión de comunicación, y donde dicha designación del primer participante como autorizado para la compartición provoca que un enlace a la clave se incluya con una invitación a la reunión para la sesión de comunicación que se envía al primer participante, la invitación a la reunión no incluye una copia de la clave; donde la experiencia de compartición de pantalla comprende una sesión de comunicación, y donde la entrada del usuario comprende la configuración del usuario de una invitación a la sesión de comunicación; donde dicha designación del primer participante como autorizado para la compartición se basa en una membresía a un grupo del primer participante, y donde la clave es accesible para los miembros del grupo.