Google ha lanzado una nueva herramienta llamada Restore Credentials que facilita a los usuarios recuperar el acceso a sus cuentas en aplicaciones de terceros de manera segura tras cambiar a un nuevo dispositivo Android.

Integrada en la API de Credential Manager de Android, esta función busca simplificar el proceso de reemplazo de dispositivos al eliminar la necesidad de ingresar manualmente las credenciales en cada aplicación.

> *«Con Restore Credentials, las aplicaciones pueden ayudar a los usuarios a acceder rápidamente a sus cuentas en un nuevo dispositivo después de restaurar sus aplicaciones y datos desde el dispositivo anterior»,* señaló Neelansh Sahai, de Google.

El mecanismo opera automáticamente en segundo plano durante la restauración de aplicaciones y datos, permitiendo que los usuarios vuelvan a iniciar sesión en sus cuentas sin requerir pasos adicionales.

Esto es posible gracias a una clave de restauración, que en esencia es una clave pública compatible con los estándares FIDO2, como las passkeys.

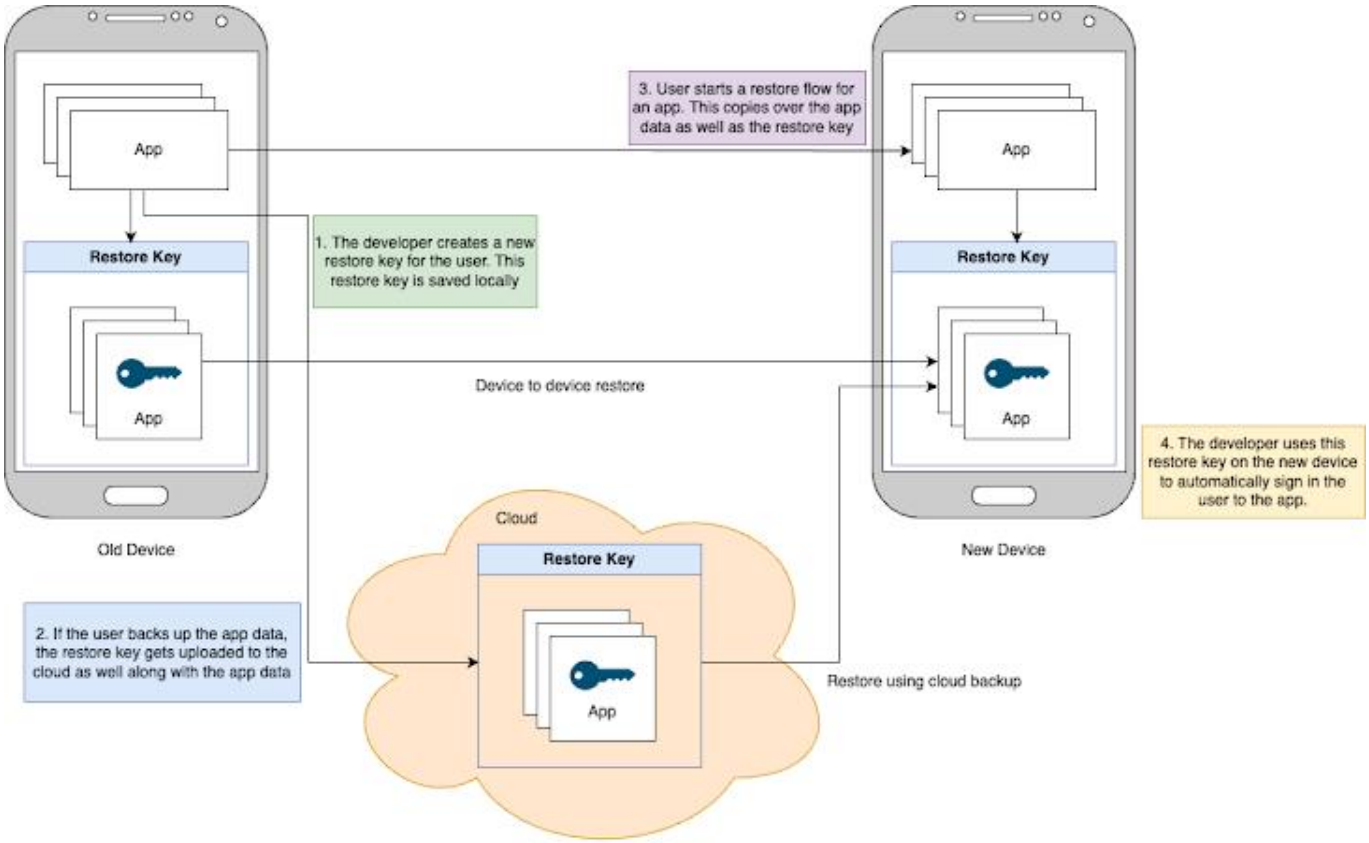
Cuando un usuario utiliza una aplicación que soporta esta funcionalidad, la clave de restauración se almacena localmente en el dispositivo mediante el Credential Manager y se cifra para mayor seguridad. Si el usuario tiene habilitadas las copias de seguridad en la nube, también puede almacenarse allí de forma cifrada.

En caso de que el usuario migre a un nuevo dispositivo y restaure las aplicaciones, las claves de restauración se recuperan automáticamente, lo que permite iniciar sesión en las cuentas sin necesidad de ingresar las credenciales nuevamente.

> *«Si el usuario autenticado actual es de confianza, puedes crear una clave de*

> *restauración en cualquier momento posterior a su inicio de sesión en tu aplicación. Por ejemplo, esto podría suceder inmediatamente después del inicio de sesión o durante una verificación de la existencia de una clave de restauración»,* explica Google a los desarrolladores.

Google también recomienda a los desarrolladores eliminar la clave de restauración en cuanto el usuario cierre sesión, para evitar que se produzcan inicios de sesión no deseados tras cerrar sesión de manera intencional.



Cabe resaltar que Apple ofrece una funcionalidad similar en iOS, utilizando un atributo denominado kSecAttrAccessible, que controla el acceso de las aplicaciones a las credenciales

almacenadas en el iCloud Keychain.

> *«El atributo kSecAttrAccessible permite determinar la disponibilidad de un elemento en función del estado de bloqueo del dispositivo»,* detalla Apple en su documentación.
>
> *«Asimismo, permite decidir si un elemento puede restaurarse en un nuevo dispositivo. Si el atributo termina con ThisDeviceOnly, el elemento solo podrá ser restaurado en el dispositivo que creó la copia de seguridad y no será transferido al restaurar los datos en otro dispositivo».*

Este lanzamiento coincide con la llegada de la primera Vista Previa para Desarrolladores de Android 16, que incluye una versión actualizada del Privacy Sandbox en Android, junto con un Privacy Dashboard mejorado, que ahora muestra qué aplicaciones han accedido a permisos sensibles en los últimos siete días.

Además, llega poco después de la publicación del nuevo Android Security Paper, un documento que describe las herramientas de seguridad integradas en el sistema operativo, como protección antirrobo, espacios privados, mecanismos de sanitización y un modo de bloqueo que restringe el acceso al dispositivo desactivando Smart Lock, el desbloqueo biométrico y las notificaciones en la pantalla de bloqueo.