La Asociación GSM (GSMA) ha anunciado oficialmente la incorporación de cifrado de extremo a extremo (E2EE) en los mensajes enviados a través del protocolo Rich Communications Services (RCS). Esto representa un gran avance en la seguridad de los mensajes compartidos entre dispositivos Android e iOS.

Para ello, las nuevas especificaciones de la GSMA para RCS incluyen E2EE basado en el protocolo Messaging Layer Security (MLS), dentro del llamado RCS Universal Profile 3.0.

> *"Las nuevas especificaciones establecen cómo aplicar MLS en el contexto de RCS. Estos procedimientos garantizan que los mensajes y otros contenidos, como archivos, permanezcan confidenciales y protegidos mientras se transmiten entre clientes»,* explicó Tom Van Pelt, director técnico de GSMA.

Con esta actualización, RCS se convertirá en el primer servicio de mensajería a gran escala en ofrecer cifrado de extremo a extremo interoperable entre diferentes aplicaciones y proveedores.

Cabe destacar que la implementación actual de RCS en la aplicación Mensajes de Google para Android utiliza el protocolo Signal para proteger las conversaciones, ya que RCS no incluía E2EE de manera nativa. Sin embargo, esta protección solo aplica a los mensajes enviados dentro de la propia app, sin extenderse a conversaciones con usuarios de iOS o clientes RCS de otros fabricantes.

Este avance llega aproximadamente seis meses después de que la GSMA anunciara su intención de reforzar la seguridad en los mensajes intercambiados entre Android e iOS. La decisión también sigue al anuncio de Apple, que confirmó que iOS 18 incluirá soporte para RCS en su aplicación de Mensajes.

En julio de 2023, Google también reveló que planea añadir compatibilidad con MLS en su servicio de Mensajes y en su implementación de código abierto de esta especificación.

> *"RCS sigue ofreciendo una variedad de funciones de mensajería interoperable entre usuarios de iOS y Android, como chats grupales, intercambio de archivos en alta resolución, confirmaciones de lectura y avisos de escritura"*, agregó Van Pelt.

En respuesta a esta actualización, Google declaró:

> *"Siempre hemos estado comprometidos con ofrecer una experiencia de mensajería segura. Los usuarios de Google Messages han contado con cifrado de extremo a extremo en RCS durante años. Nos entusiasma contar con esta nueva especificación de la GSMA y trabajaremos lo más rápido posible con el ecosistema móvil para implementarla y extender esta protección a los mensajes RCS entre plataformas."*