Aegis Authenticator es una aplicación de código abierto para dispositivos Android de Google para generar y administrar tokens de verificación de dos pasos para servicios en línea. La aplicación tiene una opción de importación, opciones de seguridad adicionales y varias características agradables que hacen que valga probar su plataforma.

Muchos servicios de Internet ya admiten la autenticación de dos factores. Es una función de seguridad opcional en la mayoría de los casos, que agrega una segunda capa de protección a los inicios de sesión de la cuenta. Los sitios aún requieren nombre de usuario y contraseña, pero también un código para completar el proceso de inicio de sesión.

Las aplicaciones de autenticación como Aegis Authenticator u opciones populares como Google Authenticator, Authy o Microsoft Authenticator, pueden generar estos códigos en dispositivos móviles. Estas aplicaciones ofrecen mejor seguridad que las opciones basadas en correo electrónico o SMS.

Twitter anunció recientemente que deshabilitará el método basado en SMS para sus usuarios gratuitos, y los usuarios pueden aprovechar la oportunidad para cambiar el método a las aplicaciones de autenticación.

Aegis Authenticator

Aegis Authenticator, como cualquier otra aplicación de autenticación, debe cumplir con ciertos estándares de seguridad. Los desarrolladores afirman que la bóveda está encriptada con AES-256-GCM y que es compatible con los estándares HOTP y TOTP de toda la industria. Es compatible con Google Auhtneticator, lo que significa que los datos pueden exportarse para Google Authenticator.

Lo que lo diferencia de las opciones más populares es que es completamente de código abierto. Los desarrolladores agregaron protecciones de contraseña y biométricas a la aplicación además de eso, lo que significa que el acceso a la base de datos está bloqueado hasta que se ingresa la contraseña.

Se pueden agregar nuevos servicios de varias formas. Además de la opción de escanear códigos QR en sitios web directamente, Aegis Authenticator admite ingresar detalles de forma manual e importarlos desde otras aplicaciones de autenticación en el dispositivo. Sin embargo, la última opción puede requerir acceso de root, que la mayoría de los usuarios de Android pueden no tener en sus dispositivos.

Se admiten las importaciones de una gran cantidad de las principales aplicaciones de autenticación. La lista incluye Authy, FreeOTP, Google Authenticator, Microsoft Authenticator, Steam e incluso, importaciones de texto del plano.

Aegis Authenticator es compatible con funciones adicionales, como grupos, funcionalidad de bloqueo automático o activación de página mediante Ripple.

Se puede descargar la aplicación en Github, en la tienda gratuita Fdroid y en Google Play. La instalación es muy sencilla desde las tres ubicaciones y no debería representar ningún problema para los usuarios de Android.

Uso de la aplicación de autenticación

Es necesario configurar una contraseña en el primer inicio de la aplicación para proteger el contenido. La aplicación muestra todos los servicios en su portada.

Es posible que los usuarios que apenas comienzan a utilizarla quieran abrir la configuración en la primera ejecución para ajustar algunos parámetros. Ahí se pueden cambiar las características de apariencia, seguridad y usabilidad. Algunas de las opciones que se encuentran allí incluyen la copia de tokens con un toque, minimizar la aplicación al copiar o habilitar la función de copias de seguridad automáticas de la aplicación.

Aegis Authenticator no sincroniza los datos con la nube de forma predeterminada. Existe una opción en la copia de seguridad para habilitar las copias de seguridad en la nube de Android.

La migración de una aplicación de autenticación a otra puede ser un proceso lento, si las

importaciones directas no están disponibles en el dispositivo. Generalmente, implica la deshabilitación de la autenticación de dos factores en el sitio web del servicio y configurarlo nuevamente.

Agregar nuevos servicios a la aplicación es un proceso rápido. Requiere escanear el código QR que muestran los sitios y servicios cuando se configura la autenticación de dos factores.