Preguntas frecuentes

¿La app MVM B·LOCK se conecta a internet?
No. La app no se conecta a internet para su funcionamiento, ni transfiere ningún dato del dispositivo ni del usuario.

¿Cómo se comunica el sistema MVM B·LOCK con mi smartphone?
El MVM B·LOCK utiliza Bluetooth para comunicarse con el smartphone y también con el mando a distancia.

¿Qué versión de Bluetooth utiliza el MVM B·LOCK?
El MVM B·LOCK utiliza Bluetooth 5, que es la última versión de este sistema.
Los dispositivos Bluetooth 4.0 y sucesivos incluyendo el actual 5 se denominan Bluetooth LE o BLE, antes llamados Bluetooth Smart.

El sistema de bloqueo para cerraduras MVM B·LOCK aporta una seguridad sin precedentes sin sustituir mi propia cerradura, pero ¿Es seguro utilizar Bluetooth?
Con la seguridad que brinda el bloqueo mecánico del MVM B·LOCK, junto con el nivel más alto de encriptación y autenticación, protección anti "sniffers", monitorización, etc., este sistema podría calificarse como uno de los más seguros del mercado.

¿Como consigue el MVM B·LOCK ese nivel de seguridad en la comunicación?
Bluetooth SIG[(1)] incorporó en la versión 4.2 una importante mejora en seguridad para proteger las comunicaciones, denominada "LESC" o "Low Energy Secure Connections" así como otras funciones y mecanismos de seguridad. Esas funciones están aprobadas y cumplen con los estándares requeridos por NIST[(2)] y FIPS[(3)].
Bluetooth SIG fomenta y promueve activamente la implementación adecuada de estas medidas de seguridad integradas en la tecnología Bluetooth.
Utilizando LESC en el MVM B·LOCK y en el smartphone, se proporciona al día de hoy el mas alto nivel de seguridad en el emparejamiento y en las comunicaciones.

¿Qué métodos y algoritmos de cifrado se añaden o mejoran en Bluetooth 4.2 y 5?
Emparejamiento: P-256 ECDH[(5)] + AES-CMAC[(6)]
Autenticación del dispositivo: AES-CCM[(7)] (HMAC-SHA-256)
Encriptación: CBC-MAC[(8)] (AES-CCM)

¿Tienen "LESC" todos los smartphones?
Apple incorporó LESC a iOS en marzo de 2015, en la versión 8.2, solo tres meses después de su publicación, por lo que en este momento cualquier iPhone actualizado es completamente compatible con las funciones de seguridad LESC.
Android lo hizo más tarde, implementándolo oficialmente en la versión 6.0, pero debido a la gran diversidad de fabricantes y sus distintas políticas de incorporación de funciones, algunos de ellos no han implementado LESC o no han publicado actualizaciones para ello.

Mi vecino tiene una cerradura con Bluetooth y un smartphone Android antiguo, y funciona sin problemas. ¿Es igual de segura?

Probablemente esa cerradura no dispone de Bluetooth 4.2 o superior, o no utiliza sus funciones avanzadas de seguridad.

Los dispositivos que utilicen protocolos de seguridad anteriores a los incorporados en Bluetooth 4.2 son de facto inseguros como revelan muchos estudios.

Muchos artículos del mercado que utilizan Bluetooth han sido desarrollados pensando en la función principal del mismo, pero no en la seguridad como una máxima, quedando en un segundo plano. Los fabricantes han preferido dar prestaciones atractivas para los usuarios a costa de reducir la seguridad. Garantizar la seguridad en las comunicaciones es prioritario.

Por ello, nuestro sistema hace uso de las capacidades de la especificación 4.2 y desaconseja el uso de versiones anteriores.

Se considera inseguro cifrar la comunicación a nivel de aplicación como lo hacen otros fabricantes, ya que es un sistema muy fácil de descifrar y reproducir, para posteriormente suplantar al usuario y acceder a la propiedad.

En la actualidad se estima que casi el 80% de los dispositivos que utilizan Bluetooth son vulnerables.

¿Y si mi smartphone Android no tiene "LESC"?

Debido a todo lo expuesto, cualquier smartphone sin esa funcionalidad no debería utilizarse.

NIST[(2)] y FIPS[(3)] solo recomiendan utilizar dispositivos que incorporen LESC.

Generalmente, en los modelos de smartphones de 2 ó 3 años, con Bluetooth 4.0 y 4.1 es posible la actualización a 4.2 mediante una actualización de software.

El fabricante es el que decide cuando proporcionar actualizaciones, y dado que LESC es una importante mejora de seguridad, hay que tener en cuenta que los dispositivos que no hayan sido actualizados para este fin tampoco habrán recibido otras actualizaciones de seguridad importantes.

Considerando las vulnerabilidades descubiertas en estos dos últimos años que afectan a Android y a otros sistemas, debería considerar firmemente dejar de utilizar su smartphone.

¿Puedo vincular mi smartphone Android al MVM B·LOCK aunque no tenga "LESC"?

Si entiende los riesgos descritos y aún así desea vincular su smartphone, hay una opción especial para ello en el menú de configuración del MVM B·LOCK.

El emparejamiento de un smartphone sin LESC o que no use el método de comparación numérica, requiere de la introducción de un número aleatorio de 6 cifras que se genera automáticamente en el momento de la vinculación con el dispositivo MVM B·LOCK. La aplicación le informará de esta opción alternativa durante la vinculación inicial, si su dispositivo no dispone de LESC.

Android

En Android, cuando instalo la app me pide que acepte unos permisos ¿Por qué?
Android requiere que el usuario acepte determinados permisos para el uso de recursos que la app necesita para su funcionamiento, como:

"¿Permitir a MVM B·LOCK acceder a las imágenes, el contenido multimedia y los archivos del dispositivo?"

La app necesita acceder al sistema de archivos para almacenar los datos de los dispositivos MVM B·LOCK del usuario. No accede a ningún otro dato ni imagen del smartphone.

"¿Permitir a MVM B·LOCK acceder a la ubicación de este dispositivo?"

Android relaciona la función de búsqueda de dispositivos Bluetooth con la ubicación, y necesita que el usuario lo autorice para que la aplicación pueda buscar un dispositivo Bluetooth. En algunos dispositivos también es necesario mantener activada la "ubicación" para un correcto funcionamiento.

"¿Permitir a MVM B·LOCK grabar audio?"

Solo en el caso de que su smartphone no disponga de LESC, se le ofrecerá una opción alternativa para vincularlo al dispositivo MVM B·LOCK que utiliza una secuencia codificada de señales acústicas para mostrar el nº PIN a introducir. La función de grabación de audio se utiliza exclusivamente en este caso, y solo para esta finalidad.

En Android, cuando voy a configurar el MVM B·LOCK y aparece "MVM B·LOCK DETECTADO" pulso en "CONTINUAR" pero no ocurre nada.
Al pulsar "CONTINUAR" aparecerá un mensaje de solicitud de vinculación Bluetooth en su smartphone, solicitando que introduzca el PIN del dispositivo a vincular. En algunos smartphones este mensaje aparece como notificación, por lo que es necesario que el usuario consulte la barra de notificaciones cuando ésta se produzca.

Acabo de vincular un MVM B·LOCK, aparece en la pantalla pero no responde.
Cuando la aplicación finalice el proceso de vinculación se cerrará automáticamente.
Espere unos segundos y vuelva a abrir la aplicación. El MVM B·LOCK estará listo para su uso.

Cuando abro la app y pulso un botón para abrir o cerrar, la aplicación se cierra sola después de un tiempo.
Una vez se ha abierto o cerrado el MVM B·LOCK, la aplicación y el MVM B·LOCK entrarán en modo bajo consumo para evitar la descarga prematura de la batería.
Para mayor comodidad para el usuario, la aplicación se cierra automáticamente al cabo de un tiempo establecido. El tiempo para activar el modo de bajo consumo puede ser configurado en el menú - configuración general - temporizador modo bajo consumo. Existe la posibilidad de ajustar de forma independiente el tiempo desde que se detecta un MVM B·LOCK y el tiempo desde que se pulsa un botón.

iOS

Cuando abro la app y pulso un botón, aparece el mensaje "MODO DE BAJO CONSUMO ACTIVADO" después de un tiempo.

Una vez se ha abierto o cerrado el MVM B·LOCK, la aplicación y el MVM B·LOCK entrarán en modo bajo consumo para evitar la descarga prematura de la batería.

El tiempo para activar el modo de bajo consumo puede ser configurado en el menú - configuración general - temporizador modo bajo consumo. Existe la posibilidad de ajustar de forma independiente el tiempo desde que se detecta un MVM B·LOCK y el tiempo desde que se pulsa un botón.

(1) Bluetooth SIG: Bluetooth Special Interest Group
(2) NIST: National Institute of Standards and Technology
(3) FIPS: Federal Information Processing Standard
(4) ECDH: Elliptic Curve Diffie-Hellman
(5) AES-CMAC: Advanced Encryption Standard - Cipher-based Message Authentication Code
(6) AES-CCM: Advanced Encryption Standard - Counter with CBC-MAC
(7) CBC-MAC: Cipher Block Chaining - Message Authentication Code (CMAC)