Technical Note

Brivo Mobile Pass (BMP) & Brivo Readers FAQ - 09/17/2018

Overview

Brivo's mobile credential, Brivo Mobile Pass (BMP), has been designed to operate with the Brivo Onair security platform. There are two primary methods by which BMP requests access: over cellular/Wi-Fi connections to the internet or over Bluetooth Low Energy (BLE) to a Brivo reader.[1] This FAQ is intended to explain the various applications and considerations in the use of Brivo Mobile Pass.

Q: How does BMP work with standard card readers and physical credentials?

The BMP mobile credential can be used to complement standard physical credentials and readers. In these situations, BMP becomes another credential associated with a User's record as if the User had been issued an additional card with the same rights as their primary card. The User's access events will be recorded in the activity log in the same way as when they use their physical card. When BMP is used to unlock a door, the light on the reader will activate as if a physical credential had been presented.

In situations where a User is using BMP with a non-BLE reader, access requests make use of the mobile device's cellular or Wi-Fi connection to communicate with Brivo Onair. Once the BMP request is authenticated, Brivo Onair instructs the panel to unlock the door.

If cellular or Wi-Fi for BMP communication is being used, the range of the credential is effectively unlimited. Onair also provides the option of limiting BMP to a local Wi-Fi connection via the Trusted Network Option which limits the range of BMP to the range of the Wi-Fi signal.

Q: How does BMP work when there is no reader at all?

The capability of Brivo Mobile Pass to communicate using cellular and Wi-Fi connections enable it to be used to control a door or gate which has no reader at all. The door or gate is simply released by BMP after direct authentication of the access request through Brivo Onair.

Q: How does BMP work with Brivo Readers?

Where Brivo Readers have been installed, the associated door can be configured for local communication between mobile devices using BMP and the Brivo Reader using BLE. In this mode, the range of BOP to the Brivo reader is typically between 3 to 6 feet for iPhones and 1 to 6 feet for Android smartphones. The exact range for a given User will vary based on the User's mobile device and environmental factors around the reader. The experience of unlocking the door is the same as it is with other readers. The User selects a door and gives the command to unlock it.

[1] Brivo readers can be used without enabling BLE in which case they operate in the same manner as other readers. For the purposes this document, Brivo assumes that when Brivo readers are mentioned, they have been configured for BLE use unless otherwise stated.

Q: Why is using Brivo Mobile Pass more secure than traditional cards?

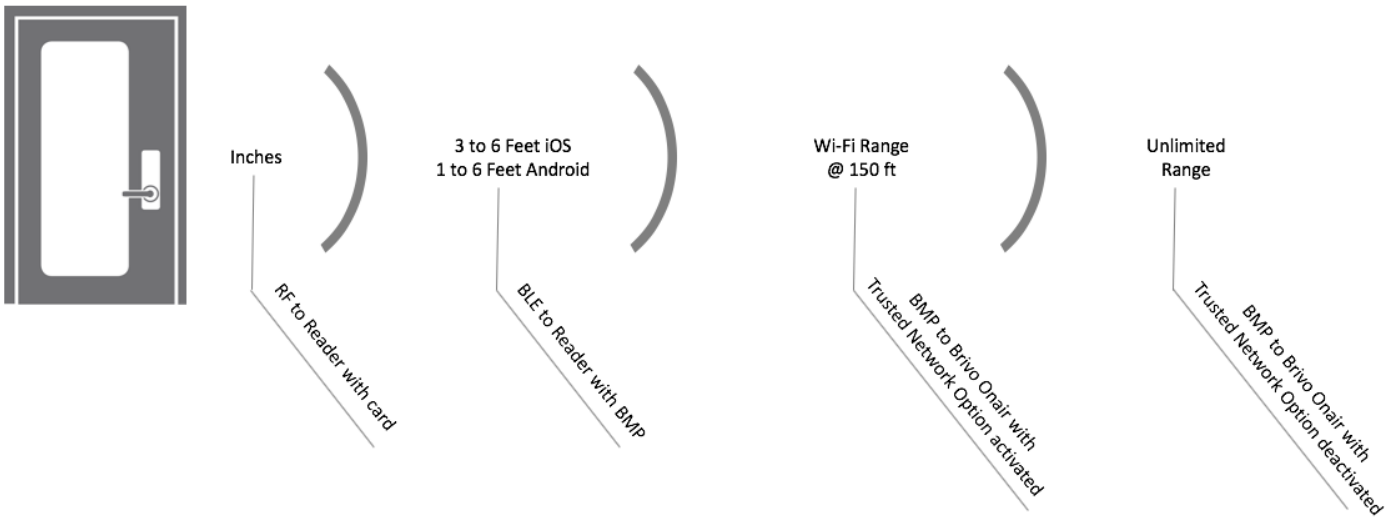
The first layer of security for BMP is the phone itself. Brivo recommends that Users lock their phones to prevent unauthorized use of their credentials. The BMP credential itself is delivered as a single-use token which is stored in the secure area of the phone. This credential cannot be transferred to another user or another mobile device. Brivo Mobile Passes can be revoked at any time by an application administrator. Brivo Onair permissions for particular doors or schedules can be modified at any time and these changes are typically effective within seconds at the panel level.

Each transmission of the mobile credential to the reader is unique and only valid for a short period of time. The Brivo Mobile Pass credential is communicated to the reader using a FIPS 202-compliant SHAKE128 cryptographic hash. This hashed value contains a timestamp which must match across the mobile device, panel, and Brivo Onair servers in order to be valid. The panel will allow access only after validating the hashed value and the User's rights at that door. Creating a unique transaction for each access request enhances security in a manner similar to the methods used to authenticate credit card payments.

Q: What kind of read range is possible with the different credential options?

The read range of any wireless technology is dependent on the installation environment and the devices involved. The graphic below provides average ranges for various types of credentials. Keep in mind that the actual ranges in an environment will vary depending on the construction, other wireless interference, and the mobile devices being used.

When installing Brivo readers, be aware that BLE signals are omnidirectional. The Brivo reader should always be installed using the supplied metal backplate to limit the ability for Users to activate a Brivo reader from within the secured location.



Note: Distances are typical and are impacted by the mobile device and installation environment.

Q: What differences can I expect if I have a mixed environment with both Brivo Readers and readers from other manufacturers?

Brivo readers enable a local BLE connection between the BMP application on a mobile device and the Brivo reader. When the door button is activated in BMP with a Brivo reader, the reader creates a connection over BLE to the User's mobile device to accept the User's credential. Brivo readers will flash while data is transmitting between the device using Brivo Mobile Pass and the reader. The credential is passed to the reader over BLE and the reader then sends that credential to the panel for an access control decision. For this to work, the mobile device must be close enough to the Brivo reader to create the BLE connection. The distance of this connection can vary from a few inches to a few feet depending on the physical environment, the type of mobile device, and the OS version of the device.

In the Brivo Onair configuration, the application administrator must choose between operating modes for a Brivo reader. Once a local BLE connection is designated for the reader, it will only function in that manner. It will not make use of Wi-Fi or cellular communication. This has advantages in areas where Wi-Fi or cellular communication is difficult or impossible such as elevators, basements, solid-metal enclosures, etc. However, BMP will work from much longer distances when not communicating over BLE.

Feature	Brivo (BLE Mode)	Other Readers
Read Time	Generally less than 1 second	Generally less than 1 second
Connection Type	Local: Device to reader	Remote: Device to cloud
Read Distance	Short: Inches to a few feet	Can be unlimited or Wi-Fi range[2]
Green Feedback	Upon successful transmission between BMP and reader	Upon access granted by the panel
Orange Feedback	Upon unsuccessful transmission between BMP nd reader	Upon access denied by the panel

Q. What differences should I expect between different phones and mobile operating systems?

Brivo has observed that many Android devices seem to have lower BLE power levels than iOS devices, resulting in shorter read ranges between BMP and the Brivo readers.

Because of a limitation with the Android operating system, Brivo Mobile Pass enforces a 20 second delay between unlock requests to Brivo readers. During this period, subsequent unlock requests to the Brivo readers will not work. This restriction is required to prevent Android devices from "locking up" the reader and preventing other devices from connecting. As a result, an Android User's first attempt to unlock the door fails, the User will need to wait 20 seconds to try again.

[2] Limited to Wi-Fi when using our Trusted Network Option