



Unified Mobile Access Solution

Security Overview

BioConnect Security Promise

1. Your card numbers never leave your on-premise device.

2. The on-premise hardware uses a zero-trust protocol with the BioConnect cloud, to ensure that the information related to card access events cannot be forged, delayed, replayed, reordered or forwarded between access points.
3. BioConnect has no access to the on-device encryption keys.

4. All authentication requests must start at your door, ensuring auditability and secure access, beyond what is offered by traditional Wiegand-based systems.

On-Prem vs Cloud Data

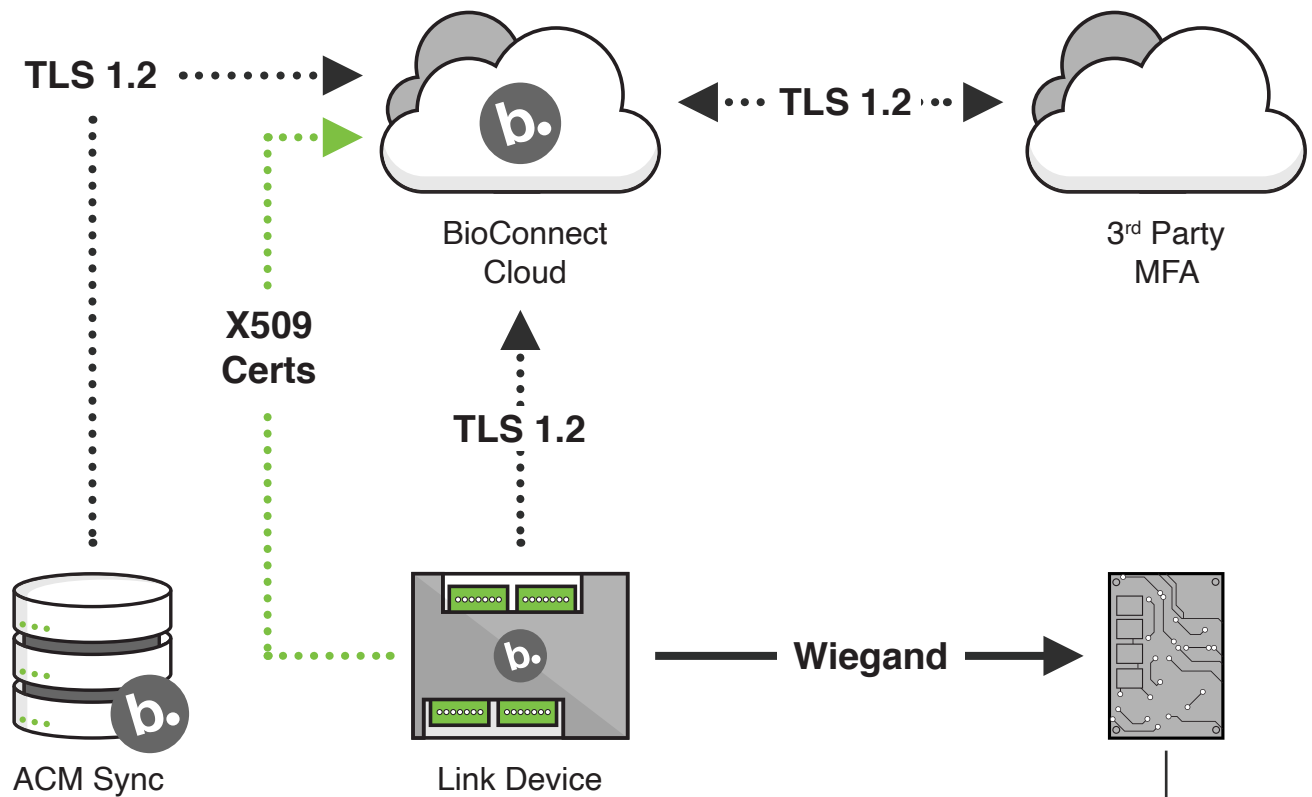
BioConnect treats your data confidentially and ensures that we use the highest levels of security in all aspects of our product. As an additional layer of privacy, we ensure only the minimum amount of data required is sent to the cloud. No raw card information or other sensitive PII will be sent to BioConnect. See right how the example user data will translate between on-premise and cloud.

Attribute	On-Premise	Cloud
First Name	John	John
Last Name	Doe	Doe
AD Username	Jdoe	Jdoe
Card Number	12345	HMAC-SHA256
Card Status	Active	Active




Architecture

The simplified architecture below shows some of the communication protocols between the various components of this solution.

Note that we ensure all communication uses mutually authenticated TLS 1.2 and your BioConnect Link provisioning is done securely using X509 certificates.



Legend

-  Device Provisioning
-  HTTPS Communication
-  BioConnect Component

Functionality

Components

The Unified Mobile Access solution has two (2) critical components to ensure that its functionality maintains the highest level of security with privacy for your enterprise.

1. BioConnect Link Cloud Service

Operates behind HTTPS, using TLS 1.2 and provides a standard web application to administer the solution, for example, adding users, schedules, devices, and cards. Our software uses a microservice infrastructure to follow modular software design principles, allowing for higher manageability and scalability. Our cloud service has been designed to scale horizontally, and vertically as required. This is to ensure that access requests are processed regardless of failures and seamlessly handles peak traffic loads.



2. Hardware

The communication between the Link hardware and the BioConnect cloud service is protected using mutually authenticated TLS 1.2 certificates on a secure MQTT protocol.

Our hardware has eight layers of redundancy to ensure your access events go through, even in the event of one or more of power, hardware or software failure. These nine layers of redundancy are:

1. Mechanical bypass to ACM in loss of power to the hardware device.
2. Device bypass to ACM if hardware device loses internet connection or cannot connect to the BioConnect cloud service.
3. Hardware equipped with partition to load an older OTA config/Firmware.
4. Multi region deployment.
5. Cloud redundancy for each service for BioConnect Link hardware device.
6. 2 independent watch dog services on the monitoring the firmware on the BioConnect Link.
7. 2 Independent watch dog services for the BioConnect Link hardware.

BioConnect Link has a dedicated hardware watchdog and software watchdog; either of these will completely reboot and reinitialize the Wiegand circuitry within 250ms of detecting a hardware or software error.

Operating Systems

The device has no traditional operating system and has undergone extensive hardening. Lack of a traditional operating System helps protect against exploiting traditional methods to gain access to the device or its services.

- No open network ports.
- No open physical ports.
- No file system.
- No unneeded processes or services.
- No command prompts.
- No ability to log in (locally or remotely).

Firmware

Hardware enforcement policies ensure that the device bootloader cannot be replaced either locally or over-the-air, even during upgrades.

The device maintains two firmware partitions and will automatically fail back to the previous valid firmware image if a corrupted or improperly signed firmware image attempts to run.



Storage

1. Data in Transit:

Each device is securely provisioned with a X509 certificate, and BioConnect does not have access to the device's locally generated private key.

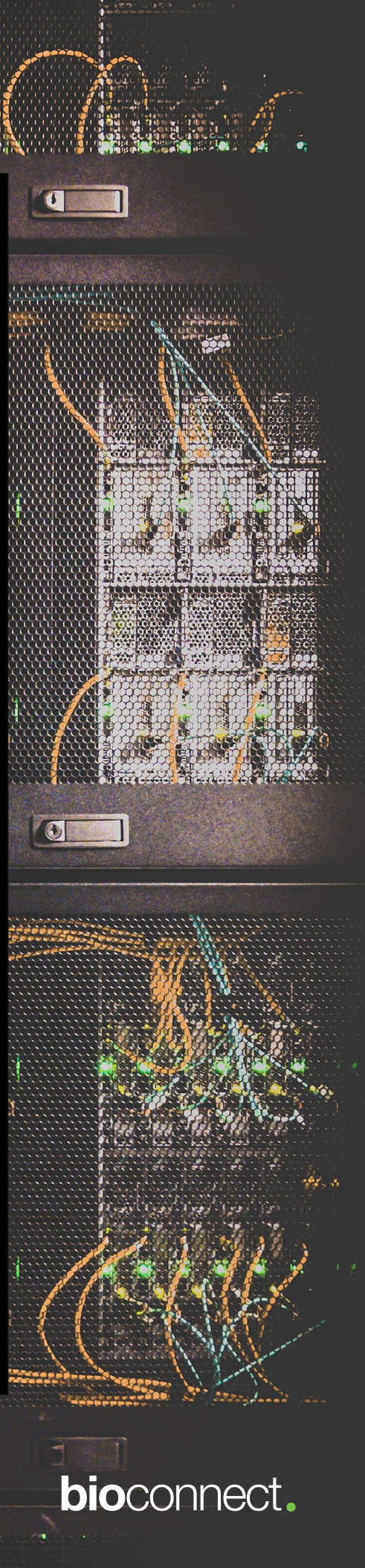
For a device, certificate-based authentication is the sole method of logging into the BioConnect cloud exchange; there are no generic usernames or pre-shared passwords that could be obtained by a third-party and then used to forge a connection to your cloud service.

In addition to the encrypted transport layer, all user physical access data is separately protected, using either strong symmetric encryption or anonymized using one-way secure hashing. (HMAC-AES256) before it leaves the device.

2. Data at Rest:

All local flash memory is protected by hardware encryption (AES-256), using a random key that is generated locally on each device and securely stored in a dedicated hardware enclave.

Over-The-Air configuration upgrades support full, automatic rollback in the event of configuration errors.



Trusted By Leading Organizations



bioconnect.



See a Solution that fits your Needs?
BioConnect can Help.

www.bioconnect.com