Reduce Risk at the Door and Cabinet with

**LR1 “Swiss Army Knife” Device & Authentication Platform**

For changing threat levels of Low - High security access points including Data Centers, Server Cabinets, Safes, MDF/IDF Closets, Doors and IIOT devices.

- **Unify Digital and Physical Authentication**
  One single identity across the Enterprise.

- **Threat Model Authentication (Dynamic Authentication)**
  Ability to adjust authentication level to match risk level.

- **‘Swiss Army Knife’ Flexibility**
  Platform provides 5 basic methods of authentication (Finger on Device, Card, Mobile Face, Mobile Yes/No Approval, Wellness Declaration).

- **Smart, Rules-Based Access**
  With custom configuration for security administration and the ability to set schedules for additional security levels, like after-hours access.

- **Deny Untrustworthy and Falsified Access**
  Key cards and FOBs can be easily duplicated. With the Link solution, suspicious access events can be blocked.

**How it works**

1. Tap your card or place your finger on the LR1
2. If Two-Factor Authentication is enabled, receive a mobile push notification and authenticate.
3. Access to door approved!
Key Features

#1  “BioConnect Link Open Protocol” powers Threat Model/Dynamic Authentication

#2  Integrated into 60%+ of the top Certified MFA Vendors
    Including DUO, Ping ID, OKTA, BC Mobile and SMS

#3  Integrated into 80%+ of the top Access Control Manufacturers

#4  Multi Class Card Reader
    Prox, iClass, MiFare, etc..

#5  BioConnect Brand Promise

Use Cases

- Data Center Cabinets
  - Auditing & Reporting
  - Cost-effective
  - Built for scale
  - Mobile biometric option

- IDF/MDF Closets
  - Flexible auth methods
  - Auditable access
  - High level of security
  - Integrates with any existing Wiegand device

- Entryways
  - After hours access
  - Remote onboarding with biometrics
  - Health reporting/HR integration

- Remote Locations
  - Remote management
  - Remote contractor
  - Remote approval
  - Biometric authentication
**Threat Model Authentication**

*Suite of “Swiss Army Knife” Options with Contactless Mobile + Wellness Authentication*

In this scenario, a user would receive a survey on their BioConnect Mobile application to provide compliance on any specific topic the customer is concerned about, for example, health, or security. Link can then approve or deny access based on the survey response, as well as alert the necessary parties.

**Dynamic Threat Responses**

Link can increase security measures required for physical access authentication based on perceived system risk. System responses can be categorized from a Low threat level to a Severe threat level as seen below.

<table>
<thead>
<tr>
<th>Low Trust / Safety</th>
<th>High Trust / Safety</th>
</tr>
</thead>
<tbody>
<tr>
<td>MultiClass Card Authentication</td>
<td>IT Approved MFA via Mobile Authentication at the Door</td>
</tr>
<tr>
<td>Wellness Declaration Authentication</td>
<td>Touchless Multi-Factor Mobile Face Authentication</td>
</tr>
<tr>
<td>On-Device Finger Authentication</td>
<td></td>
</tr>
</tbody>
</table>

**Survey Declaration as Authentication**

In this scenario, a user would receive a survey on their BioConnect Mobile application to provide compliance on any specific topic the customer is concerned about, for example, health, or security. Link can then approve or deny access based on the survey response, as well as alert the necessary parties.
Mobile Authentication Methods

Yes/No Authentication
Simple yes/no mobile authentication using our BC Mobile app or one of our supported Authenticators.

Wellness Declaration
Protect the safety of your people and environments with Mobile Wellness Declaration.

Mobile Biometric Authentication
Add a layer of security by enabling mobile biometric authentication using facial recognition.

Supported Authenticators

Use biometric facial recognition or a simple ‘Approve’/’Deny’ to authenticate.
The LR1 setup is exactly the same as a regular biometric reader connected to BioConnect Enterprise.

Once the reader gets an authentication request (Finger tap/card scan) it reaches out to your local Bioconnect server where the card number is converted to human identity.

If device is enabled for additional mobile verification, BioConnect cloud will reach out to the user for them to verify their identity out-of-band via their mobile phone (via BC Mobile or an existing third-party MFA solution).

BioConnect gathers data (for the Insights feature) and can layer additional safeguards onto the transaction.

If approved, the transaction is let through.

Solution Architecture

#1 The LR1 setup is exactly the same as a regular biometric reader connected to BioConnect Enterprise.

#2 Once the reader gets an authentication request (Finger tap/card scan) it reaches out to your local Bioconnect server where the card number is converted to human identity.

#3 If device is enabled for additional mobile verification, BioConnect cloud will reach out to the user for them to verify their identity out-of-band via their mobile phone (via BC Mobile or an existing third-party MFA solution).

#4 BioConnect gathers data (for the Insights feature) and can layer additional safeguards onto the transaction.

#5 If approved, the transaction is let through.

Unifying Digital and Physical Access with Touchless Access

Card tap acts as your ‘USERNAME’

A card alone does not prove an identity, it simply provides an identifier, similarly to a username.

Mobile Authentication acts as your ‘PASSWORD’

The mobile authentication acts as the password by proving the user is who they say they are.
The BioConnect Enterprise Access Control Software is integrated with the BioConnect Link Mobile Multi-Factor Authentication system. Now, you can manage and configure your LR1 and other biometric devices for reliable, touchless authentication all from one place, with the power of BioConnect Link.

Device and Authentication Management All in One Place.

Manage and configure your LR1, Suprema Devices, and Mobile Authentication Enabled Devices, all from one location.

 Seamlessly Integrate into Your Access Control System

No need to import users or manually update information, simply follow the setup guide to connect to your ACM to pull the necessary details.

Securely Connect to the Cloud

Your critical information stays on premise, to provide the convenience of cloud with the security benefits of on-premise.
<table>
<thead>
<tr>
<th>Product Code</th>
<th>Product Name</th>
<th>Product Details</th>
</tr>
</thead>
<tbody>
<tr>
<td>BC-LR1</td>
<td>LR1</td>
<td>LR1 Biometric Hardware Device</td>
</tr>
</tbody>
</table>

### BioConnect Link Platform + LR1 Details

<table>
<thead>
<tr>
<th>Details</th>
<th>LR1</th>
</tr>
</thead>
<tbody>
<tr>
<td>Brand Promise</td>
<td>Enterprise Security, Personal Privacy &amp; Safety, Delivered Simply and Reliably</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Details</th>
<th>LR1</th>
</tr>
</thead>
<tbody>
<tr>
<td>Enhanced Enterprise Security</td>
<td>Threat Model Authentication Set Based on Changing Threat Level</td>
</tr>
</tbody>
</table>

**“Swiss Army Knife” Authentication Platform**

- **Digital Multi-Factor Authentication (MFA)**
- **Configurable for Touchless Security**
- **Human Trust (Face Recognition)**
- **Declaration Survey Authentication**

**Software Architecture**

- On Premise + Cloud Connection

### LR1 Specifications (Link Reader Outdoor/Indoor) Rated Hardware

<table>
<thead>
<tr>
<th>Details</th>
<th>LR1</th>
</tr>
</thead>
<tbody>
<tr>
<td>Link Protocol</td>
<td>Embedded</td>
</tr>
<tr>
<td>Interfaces/RF Options</td>
<td>Wiegand, RS485, OSDP, V2.1.6, TTL I/O, 1 Relay</td>
</tr>
<tr>
<td>Multi Card Devices</td>
<td>BLE</td>
</tr>
<tr>
<td>Multi Card Readers</td>
<td>125KHz EM/HID Prox, 13.56 MHz MiFare, DESFire (EV1), Felica/NFC/iClass SE/SR/Seos</td>
</tr>
<tr>
<td>Biometric</td>
<td>Fingerprint</td>
</tr>
<tr>
<td>Sensor type</td>
<td>Optical Sensor (OPS)</td>
</tr>
<tr>
<td>Accuracy &amp; Security</td>
<td>Advanced LFD Technique</td>
</tr>
<tr>
<td>Max. Users</td>
<td>500,000 (1:1), 100,000 (1:N)</td>
</tr>
<tr>
<td>Max. Template</td>
<td>1,000,000 (1:1), 200,000 (1:N), (1 finger = 2 templates)</td>
</tr>
<tr>
<td>Max. Logs</td>
<td>1,000,000 (text)</td>
</tr>
<tr>
<td>Performance</td>
<td>CPU 1.2 G Hz, Quad Core</td>
</tr>
<tr>
<td>Memory</td>
<td>2GB Flash + 256 MB RAM</td>
</tr>
<tr>
<td>Template</td>
<td>SUPREMA; ISO-19794-2, ANSI 378</td>
</tr>
<tr>
<td>Extractor/Matcher</td>
<td>MINEX Certified and Compliant</td>
</tr>
<tr>
<td>Ingress Protection</td>
<td>IP67</td>
</tr>
<tr>
<td>Impact Protection</td>
<td>IK09</td>
</tr>
<tr>
<td>LFD</td>
<td>Supported</td>
</tr>
<tr>
<td>PoE</td>
<td>Supported (IEEE 802.3af compliant)</td>
</tr>
<tr>
<td>Tamper Proof</td>
<td>Supported</td>
</tr>
<tr>
<td>LED</td>
<td>Multi-Color</td>
</tr>
<tr>
<td>Power</td>
<td>Voltage: DC 12V Current Max. 600mA</td>
</tr>
<tr>
<td>Operating Temperature</td>
<td>-20 C to 50 C</td>
</tr>
<tr>
<td>Humidity</td>
<td>0% ~ 80%, Non-condensing</td>
</tr>
<tr>
<td>Dimensions (WxHxD, mm)</td>
<td>50 x 172 x 43.5</td>
</tr>
<tr>
<td>Weight</td>
<td>251g (294g incl. bracket, washers, bolts)</td>
</tr>
<tr>
<td>Certificates</td>
<td>CE, FCC, KC, RoHS, REACH, WEEE</td>
</tr>
</tbody>
</table>

© 2020 BioConnect
Security & Privacy

Hardware: BioConnect Link Device

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 multiple layers of redundancy to ensure your access events go through, even in the event of one or more of power, hardware or software failure.

1. Mechanical bypass to ACM in case of 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. Cloud redundancy for each service for BioConnect Link hardware device.
5. 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.

Software: BioConnect Link Admin Console

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.

Privacy and Data 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.