

## **SECTION 28 13 00 – BIOMETRIC READER DEVICE**

### **BioConnect® Arc Vision™ AI-Powered Facial Authentication Reader**

#### **Reference Engineering Specification**

Based on BioConnect Arc Vision product documentation and published specifications.

This specification is intended for use by Architects and Engineers (A&E) as a basis-of-design biometric reader specification and may be adapted to suit project-specific requirements.

---

### **PART 1 – GENERAL**

#### **1.1 SUMMARY**

A. Section includes requirements for a wall-mounted, contactless biometric facial authentication reader designed for use within a physical access control system (PACS).

B. Reader shall utilize advanced, on-device artificial intelligence to perform facial recognition authentication with high accuracy and rapid response.

C. Reader shall support multiple contactless credential types and privacy-centric enrollment methods while interfacing with an upstream Physical Access Control System (PACS).

D. Reader shall be suitable for indoor and outdoor installations, including high-traffic commercial, enterprise, and perimeter access points.

---

#### **1.2 SYSTEM DESCRIPTION**

A. The biometric reader shall be a self-contained, network-capable facial authentication device performing local (edge-based) facial template matching.

B. The reader shall incorporate dedicated AI processing hardware to execute facial recognition algorithms directly at the device.

C. The reader shall operate as a peripheral authentication device, presenting credential data and authentication results to an access control panel or biometric middleware using standard signaling interfaces.

D. The reader shall support centralized configuration, enrollment, monitoring, and firmware management via manufacturer-supported software platforms.

---

### **1.3 PERFORMANCE REQUIREMENTS**

- A. Reader shall provide fast and accurate facial authentication suitable for high-throughput access points and modern enterprise environments.
- B. Reader shall support controlled-range facial authentication optimized for door-level access control.
- C. Reader shall accurately authenticate users under varying real-world conditions, including changes in appearance such as eyewear, facial hair, or headwear, subject to policy configuration.
- D. Reader shall incorporate live-face detection to mitigate spoofing attempts using photographs, video displays, or other presentation attacks.

---

### **1.4 SUBMITTALS**

- A. Manufacturer's product data and technical specifications.
- B. Installation instructions, wiring diagrams, and mounting guidelines.
- C. Environmental ratings, impact resistance, and regulatory compliance documentation.
- D. Description of supported credential types and enrollment workflows.

---

### **1.5 QUALITY ASSURANCE**

- A. Manufacturer shall specialize in enterprise-grade biometric authentication technologies with a focus on privacy and data protection.
- B. Reader shall be listed and certified for use in commercial, enterprise, and regulated-market access control installations.
- C. Reader firmware, biometric algorithms, and AI processing models shall be supplied and maintained by the original equipment manufacturer.

---

### **1.6 WARRANTY AND SUPPORT**

- A. Biometric reader shall be covered by the manufacturer's standard hardware warranty.

B. Manufacturer shall provide technical support, firmware updates, and security enhancements throughout the supported lifecycle.

---

## **PART 2 – PRODUCTS**

### **2.1 BIOMETRIC FACIAL AUTHENTICATION READER**

A. Basis of Design: **BioConnect Arc Vision™** AI-powered facial authentication reader.

B. Manufacturer: BioConnect (or approved equal).

---

### **2.2 AUTHENTICATION AND CREDENTIAL FEATURES**

A. Reader shall support the following contactless authentication methods:

1. Facial recognition with on-device AI processing.
2. Contactless smart-card credentials.

B. Reader shall support multi-factor authentication combining facial recognition with additional contactless credentials when required.

C. Reader shall provide user feedback via integrated display, multi-color LED indicators, and audible annunciation.

---

### **2.3 FACIAL RECOGNITION TECHNOLOGY**

A. Reader shall integrate multiple cameras, including visible-light and infrared imaging, to support accurate facial authentication.

B. Facial template generation and matching shall be executed locally at the reader without reliance on real-time cloud processing.

C. Reader shall support adaptive facial recognition techniques to maintain accuracy over time.

D. Reader shall include live-face detection and anti-spoofing mechanisms to protect against fraudulent authentication attempts.

---

### **2.4 PRIVACY AND DATA PROTECTION**

A. Reader shall support privacy-by-design principles, minimizing storage and exposure of biometric data.

B. Reader shall support automated enrollment workflows leveraging existing profile images from PACS or identity systems where permitted by policy.

C. Reader shall support privacy-preserving credential options that allow biometric templates to be stored under user control where applicable.

---

## **2.5 PROCESSING AND MEMORY**

A. Reader shall include an embedded multi-core processor with dedicated AI or neural processing acceleration.

B. Reader shall include onboard memory sufficient to support enterprise-scale facial templates, credential records, and event logging.

---

## **2.6 INTERFACES AND COMMUNICATIONS**

A. Reader shall support the following interfaces:

1. Ethernet (10/100/1000 Mbps) for TCP/IP communication.
2. Wireless networking where supported by the device configuration.
3. Wiegand input and output.
4. RS-485 communications supporting host or slave operation, including OSDP.
5. Relay output for lock and door hardware control.

B. Reader shall support deployment in both:

1. Network-connected biometric architectures, and
  2. Panel-connected reader architectures using standard access-control signaling formats.
- 

## **2.7 ELECTRICAL REQUIREMENTS**

A. Reader shall operate on low-voltage DC power supplied by a listed and regulated power source.

B. Reader shall support Power over Ethernet (PoE or PoE+) where specified by the manufacturer.

C. Reader relay outputs shall be suitable for interfacing with electric strikes, magnetic locks, and access-controlled hardware via external power supplies.

---

## **2.8 ENVIRONMENTAL AND DURABILITY REQUIREMENTS**

A. Reader enclosure shall be rated for outdoor use with an ingress protection rating appropriate for exterior installations.

B. Reader shall provide vandal-resistant construction suitable for commercial and public environments.

C. Reader shall be designed for reliable operation across exterior temperature and humidity ranges.

---

## **2.9 PHYSICAL CHARACTERISTICS**

A. Reader shall feature a slim, modern form factor suitable for mullion or surface mounting.

B. Reader enclosure shall be constructed of durable, impact-resistant materials.

C. Reader shall incorporate internal tamper detection to identify unauthorized removal or opening.

---

## **2.10 SYSTEM COMPATIBILITY**

A. Reader shall be compatible with enterprise PACS platforms through direct panel interface or biometric middleware, including but not limited to:

1. Genetec Security Center.
2. Software House C•CURE 9000.
3. LenelS2 OnGuard / NetBox.
4. AMAG Symmetry.
5. Acre Security (Open Options and RS2).

6. Brivo.

7. Other systems supporting standard reader interfaces.

B. Reader shall not require proprietary access-control panels when standard signaling interfaces are utilized.

---

## **PART 3 – EXECUTION**

### **3.1 INSTALLATION**

A. Install reader in accordance with manufacturer installation instructions, mounting templates, and applicable codes.

B. Position reader to ensure appropriate facial capture distance, viewing angle, and unobstructed user approach.

C. Provide weather-sealed mounting and conduit terminations for exterior installations.

---

### **3.2 CONFIGURATION**

A. Configure reader communication protocols and network parameters to match system design.

B. Configure authentication modes, display behavior, LED indicators, and relay timing per project requirements.

C. Integrate reader with centralized enrollment and management platforms where applicable.

---

### **3.3 TESTING AND COMMISSIONING**

A. Verify facial authentication accuracy, response time, and anti-spoofing behavior.

B. Verify credential signaling and integration with the PACS.

C. Verify tamper detection, environmental sealing, and door hardware operation.

---

### **3.4 TRAINING AND HANDOVER**

A. Provide administrator and technician training on facial enrollment workflows, privacy features, and reader operation.

B. Deliver as-built documentation, configuration records, and manufacturer manuals to the Owner.

---

**END OF SECTION 28 13 00 – BIOMETRIC READER (BIOCONNECT ARC VISION)**