SECTION 28 13 00 – BIOMETRIC ACCESS CONTROL SYSTEM (MIDDLEWARE)

Reference Engineering Specification

Based on BioConnect Enterprise Software v5.5 architecture, installation, configuration, and published Privacy & Compliance practices (April 2025).

This specification is intended for use by Architects and Engineers as a basis-of-design and may be adapted to suit project-specific requirements.

PART 1 – GENERAL

1.1 SUMMARY

A. Section includes requirements for a biometric authentication **middleware** platform that integrates biometric readers with the Owner's Physical Access Control System (PACS).

B. The system shall provide centralized biometric enrollment, device management, credential synchronization, authentication enforcement, and privacy controls while presenting standard Wiegand or OSDP signals to upstream access control panels.

C. System shall support multi-modal authentication including fingerprint, facial recognition, card, PIN, and combinations thereof, subject to hardware capabilities.

D. System shall incorporate **privacy-by-design principles**, including consent enforcement, encryption, data minimization, and auditable biometric lifecycle management.

1.2 SYSTEM DESCRIPTION

A. The biometric system shall consist of:

1. On-premises biometric middleware server software.
2. Biometric reader devices connected via TCP/IP.
3. Integration services to synchronize cardholder and credential data with the PACS.
4. Biometric templates and metadata stored centrally and/or locally at devices, depending on biometric modality.

B. Biometric middleware shall not replace the PACS, but shall operate strictly as an authentication and credential presentation layer.

C. Communication to control panels shall occur using Wiegand or OSDP formats configured to match PACS requirements.

D. Middleware architecture shall minimize exposure of biometric data by avoiding unnecessary storage, replication, or downstream distribution.

1.3 PERFORMANCE REQUIREMENTS

A. Automatic synchronization of users and devices shall occur at scheduled intervals without manual intervention.

B. Manual synchronization mechanisms shall be provided for:

1. User data.
2. Device data.
3. Location-based device groups.

C. Facial authentication systems shall perform biometric matching locally at the device and shall not rely on real-time server-side matching.

1.4 SUBMITTALS

A. Product data for biometric middleware software.

B. System architecture diagram showing:

1. PACS integration.
2. Middleware server and database.
3. Biometric devices.
4. Network and security boundaries.

C. Network port, firewall, and encryption requirements.

D. Supported PACS platforms and software versions.

E. Description of consent tracking, biometric data handling, and audit capabilities.

1.5 QUALITY ASSURANCE

A. Manufacturer shall be regularly engaged in the design and development of biometric authentication middleware solutions for regulated environments.

B. Middleware shall support enterprise-grade deployment models including standalone and distributed (MAS/SAS) architectures.

C. Installation and configuration shall be performed in accordance with manufacturer documentation and published privacy-compliance guidance.

1.6 WARRANTY AND SUPPORT

A. Software support shall include installation, configuration, privacy feature configuration, and troubleshooting assistance.

B. Manufacturer shall provide documented support channels including telephone and online support resources.

PART 2 – PRODUCTS

2.1 BIOMETRIC AUTHENTICATION MIDDLEWARE

A. Basis of Design: BioConnect Enterprise 5.5.

B. Middleware shall provide:

1. Centralized biometric enrollment (fingerprint and facial).
2. Device provisioning, configuration, and firmware updates.
3. Credential mapping and card format management.
4. Integration with multiple PACS platforms via SDKs or APIs.
5. Privacy and compliance controls including consent enforcement, encryption, audit logging, and data minimization.

2.2 SERVER PLATFORM REQUIREMENTS

A. Operating System:

1. Windows Server 2022.

B. Database:

1. Microsoft SQL Server 2019 or later.
2. SQL Express permitted only for small, non-enterprise deployments.

C. Minimum Server Resources:

1. CPU: Dual-core x64, 2.4 GHz minimum.
2. Memory: 8 GB minimum (16 GB recommended).
3. Storage: Minimum 10 GB available.

D. Enterprise Deployments:

1. Support Master Application Server (MAS) and Satellite Application Server (SAS) architectures.
2. Separate application and database servers recommended.

2.3 NETWORK, SECURITY, AND COMMUNICATIONS

A. Biometric devices shall communicate with the middleware server over TCP/IP.

B. All communications between devices, middleware, clients, and databases shall be **encrypted in transit** using industry-standard protocols (e.g., TLS).

C. The system shall support database encryption for biometric templates, consent records, and sensitive metadata, with encryption configurable and enabled as required by the system administrator or customer in on-premises deployments.

D. Required ports shall include, but not be limited to:

1. Biometric device communication.
2. Middleware client services.
3. REST API services.
4. Licensing and configuration services.

E. PACS integration shall not require proprietary panel hardware.

2.4 AUTHENTICATION MODES

A. Supported authentication modes shall include:

1. Card + Fingerprint.
2. Fingerprint only.
3. Card only.
4. Card + PIN.
5. Multi-factor combinations as supported by device firmware.

B. Authentication mode selection shall not alter consent, audit, or privacy enforcement behavior.

C. Template-on-Card functionality shall be supported for smartcards where specified.

2.5 BIOMETRIC DATA HANDLING

A. Fingerprint templates shall be stored within the middleware database and/or device memory using encrypted storage, with encryption in the database being configurable and enabled as required by the system administrator or Owner in on-premises deployments.

B. Facial authentication shall utilize image-based enrollment for biometric provisioning, with biometric templates generated at the device and used for authentication.

C. Biometric templates shall be stored locally at the device for authentication purposes and managed by the middleware system for synchronization, configuration, and lifecycle management.

D. Enrollment images shall not be used for biometric identification or matching and shall not be retained locally at biometric devices. Enrollment images may be retained within the middleware system to support enrollment workflows, including secure distribution to authorized devices and system synchronization, and shall be subject to configurable retention, access control, and deletion policies.

E. Middleware shall support configurable biometric data retention and deletion aligned with Owner policy, system configuration, and applicable privacy regulations.

2.6 BIOMETRIC CONSENT MANAGEMENT

A. The biometric middleware shall provide an optional **consent tracking and enforcement capability** supporting privacy, regulatory, and policy-driven biometric deployments.

B. Consent Enforcement:

1. When enabled, biometric enrollment shall be blocked until valid consent is recorded.
2. Consent enforcement shall occur at the middleware layer and apply uniformly to all biometric modalities.

C. Consent Capture:

1. System shall support verification of a consent flag from an integrated external system.
2. Consent flags may be issued through an integrated external system.

D. Consent Association and Independence:

1. Consent status shall be associated with the individual record.
2. Consent records shall be stored independently of biometric templates.

E. Lifecycle Enforcement:

1. Revocation or expiration of consent shall require re-consent prior to re-enrollment.
2. Consent status shall not affect PACS card-only or non-biometric access.

F. Audit and Compliance:

1. System shall maintain auditable records of biometric enrollment, deletion, re-enrollment, and consent state.
2. Audit data shall be available for administrative review and compliance verification.

G. Regulatory Alignment:

1. Consent and privacy controls shall support compliance with biometric privacy regulations including, but not limited to, BIPA, GDPR, CCPA, and equivalent regional legislation.
2. Owner retains responsibility for defining consent language, legal policy, and regulatory interpretation; middleware provides technical enforcement and audit support.

2.7 COMPATIBLE PACS SYSTEMS

A. Middleware shall support integration with the following PACS platforms, subject to version compatibility:

1. Genetec Security Center.
2. LenelS2 OnGuard and S2 Netbox.
3. Software House C•CURE 9000.
4. AMAG Symmetry.
5. Brivo.
6. Acre (Open Options and RS2).
7. Keyscan Aurora.
8. Other systems supporting standard reader interfaces.

2.8 OPTIONAL DEEP EMBED PACS INTEGRATION

A. The biometric middleware shall optionally support a **Deep Embed integration** with supported PACS platforms, providing biometric enrollment, credential management, and audit visibility **directly within the PACS user interface**, without requiring operators to launch a separate client application.

B. Supported Platforms:

1. Genetec Security Center.
2. Software House C•CURE 9000

C. Functional Capabilities:

1. Access biometric enrollment and management functions directly within the PACS cardholder/personnel record.
2. Enroll, delete, and re-enroll fingerprint and facial biometrics using designated enrollment readers.
3. View enrolled biometric templates and enrollment status from within the PACS interface.
4. Manage card-only or biometric bypass credentials where supported by the PACS.
5. Display enrollment activity logs within the PACS operator interface for audit and troubleshooting purposes.

D. Operational Characteristics:

1. Deep Embed shall leverage the BioConnect middleware services and database for biometric processing and storage; biometric data shall not be stored directly within the PACS database.
2. Enrollment quality thresholds may be selectable during enrollment to enforce biometric capture standards.
3. Enrollment readers must be online and designated within the middleware system to be available in Deep Embed views.

E. Security and Privacy Alignment:

1. Consent enforcement, encryption, audit logging, and data retention rules defined in this Section shall apply equally to Deep Embed enrollment workflows.

F. Use Cases:

1. Streamlined biometric enrollment for security operators working exclusively within PACS environments.
2. Reduced administrative overhead by eliminating context-switching between PACS and middleware clients.
3. Improved auditability through consolidated personnel and biometric management interfaces.

G. Limitations

1. Deep Embed is limited to standalone deployments or systems using enrollment readers on the MAS. Deep Embed is not supported for SAS as of release v5.5.

PART 3 – EXECUTION

3.1 INSTALLATION

A. Install middleware server software on dedicated application server.

B. Install client software on authorized enrollment workstations.

C. Configure firewall and encryption rules per documented requirements.

3.2 CONFIGURATION

A. Configure middleware to synchronize with PACS, with appropriate access and network permissions.

B. Configure biometric devices with server IP address, communication ports, and authentication modes.

C. Configure card formats, facility codes, and bit lengths to match PACS configuration.

D. Configure consent enforcement, retention policies, and audit logging per Owner requirements.

3.3 ENROLLMENT PROCEDURES

A. Fingerprint enrollment shall capture multiple samples per finger to ensure data quality.

B. Facial enrollment may be performed:

1. Directly at supported devices, or
2. From imported images where supported by PACS integration.

C. Enrollment readers shall remain online during enrollment procedures.

D. Biometric enrollment shall not proceed without verified consent where consent enforcement is enabled.

3.4 SYNCHRONIZATION

A. Automatic synchronization shall occur at predefined intervals.

B. Manual synchronization shall be available for:

1. Users.
2. Devices.

3.5 TESTING AND COMMISSIONING

A. Verify:

1. Biometric authentication accuracy.
2. Credential presentation to PACS.

3. Consent enforcement behavior.
4. Encryption, deletion, and audit functionality.

B. Confirm enrollment, deletion, re-enrollment, and synchronization behavior.

3.6 TRAINING AND HANDOVER

A. Provide administrator training on:

1. Enrollment and consent workflows.
1. Device management.
2. Synchronization operations.
3. Privacy and audit controls.

B. Deliver system documentation and configuration records.

END OF SECTION 28 13 00 – BIOMETRIC ACCESS CONTROL SYSTEM (BIOCONNECT ENTERPRISE)