TrustPoint™
3-Factor BIO Fingerprint Reader with PKI Support

Contact or Contactless Operation with Card, PIN, BIO & Optional PKI Challenge-Response Authentication

FEATURES
- Structural Polycarbonate Housing with Stainless Steel Mounting Plate
- Weatherized for Outdoor Operation
- IP-65 Engineered
- High Intensity LED Display Provides Clear Directions for User in all Temperature Conditions
- FIPS-201 Listed BIO Scanner is Sealed Against Moisture for use in Exterior Applications
- Weatherized Keypad with Die Cast Metal Telephone Keys
- Contact Card Interface Includes Protective Shutter to Resist Foreign Objects
- Contact Interface Provides Access to the PIV Authentication Certificate and BIO-Template via FIPS-201 approved BIO Scanner
- Forward Compatible Flash Reprogrammable Technology
- Algorithm Support Includes RSA-1024, RSA-2048, SHA-1, SHA-2, AES 128 & 256, 3DES and Random Number Generation
- Reliable Contact and Contactless Operation with all Federal PIV, CAC, TWIC, FRAC & PIV-I Credentials
- Integrates with Most Brands of PACS: Field Configurable Options for PIN and Wiegand Output Formats
- Mode Authentication Function
- Supports Control from System Panel of:
  o 1-Factor Card Only
  o 2-Factor Card + PIN
  o 3-Factor Card + PIN + BIO
- Supports TWIC Compliant Privacy Key via Contact and Contactless Interface
- SECURELY ENGINEERED & MANUFACTURED by BRIDGEPOINT IN THE USA

Cyber-Secure Option:
Optional Crypto Module executes PKI Challenge-Response to Assure Credential Authenticity:

Contactless Mode: Issues Challenge to Card Auth Key (CAK). No PIN Required

Contact Mode: Issues Challenge to Personal Authentication Key (PAK). PIN Required

Verifies Digital Signature on BIO Template

Total Transaction Time: <3 Sec.
PHYSICAL ACCESS SOLUTIONS

GENERAL DESCRIPTION

TrustPoint BIO-Readers are designed to deliver security levels defined by NIST and OMB as “HIGH” (Level 3) and “VERY HIGH” (Level 4). The security level depends on the Public Key Infrastructure (PKI) authentication mechanism that is implemented.

The TrustPoint 3-Factor Dual Interface BIO-Reader supports a PKI challenge-response to the Personal Authentication Key (PAK) over the contact interface for all Personal Identity Verification (PIV) Credentials including the PIV, CAC, TWIC, FRAC and PIV-I. The user is required to enter their PIN to enable the challenge to the PAK, resulting in a 2-Factor authentication process.

The Reader also supports a challenge to the Card Authentication Key (CAK) over the contactless interface. A PIN is not required which results in a 1-Factor authentication process (NOTE: the DoD CAC and the DHS PIV credentials do not have a CAK and therefore do not support PKI on the contactless interface).

TrustPoint Readers are equipped with two high performance microcontrollers. The first is dedicated to processing the reader transaction with the credential and the biometric template and the second is dedicated to the PKI processes including the performing a challenge-response to the PIV certificate private keys.

BIOMETRIC AUTHENTICATION

Digitally signed encrypted biometric templates of the User’s right and Left index fingers are stored on the PIV credential. Accessing the template requires entry of the PIN by the User after which the TrustPoint Reader can extract the template and perform a “one-to-one” match against the “live-scan” of the Users finger. Because there is a one-to-one comparison and not a comparison of one template against a database of many templates the match is extremely fast and reliable.

In addition to matching the biometric the TrustPoint Reader also verifies the template digital signature per NIST guidance. Once the PIN is entered, the process of extracting the template and performing the match is less than 0.20 seconds.

The TrustPoint Reader is the most user-friendly biometric reader available. When the sensor is ready for a scan it lights up with a bright red glow and the LCD display guides the user through the process by presenting the following messages at each step of the authentication process:

“Insert PIV or CAC”
“Enter PIN”
“Scan Finger”
“Press 1 to Re-Scan” (if scan fails)
“Remove Card”
“Access Granted” or “Access Denied”

The Reader will also display the reason for access denied such as “BIO Failed; PKI Failed; Card not in System; etc.

The sensor is a ruggedized, high image quality fingerprint optic module with high speed NIST MINEX Compliant fingerprint matching. The module carries an IP-65 rating, is FBI Certified as meeting FBI Image Quality Specs (IQS), is compliant with FIPS 201 standard for PIV Single Finger Readers and is listed on the General Services Administration’s FIPS 201 Approved Products List (APL) for use in the Federal Government’s Personal Identity Verification (PIV) program.

HIGHLY CONFIGURABLE SECURITY MODES

All BridgePoint 3-Factor Readers can be controlled from the PACS panel to operate in any of the following authentication modes:

1-Factor Credential Only
2-Factor Credential + PIN
3-Factor Credential + PIN + BIO

Both 2-Factor and 3-Factor authentication can be implemented to increase security during off-duty hours or high threat level conditions. The mode can be configured directly in the Reader or controlled automatically or manually by the security officer. TrustPoint Readers can also be configured with the PKI Challenge-Response in the ON or OFF Mode. This feature allows the customer to use TrustPoint in Security Level I & II and later implement Level III & IV.
PHYSICAL ACCESS SOLUTIONS

SPECIFICATIONS

PART NUMBER
71-02-3222: 3-Factor Dual Interface + PIN + BIO + PKI
(NOTE: Model No. 71-02-3222 is equipped with Optional TrustPoint PKI crypto-module)

STANDARDS SUPPORTED
• ISO 7816 Card-to-Reader Interface
• ISO 14443 Contactless Card-to-Reader Interface
• ISO/IEC 7816-3 Class A Smart Card Standard
• FIPS-201
• NIST 800-73 PIV Interfaces
• NIST 800-76 Biometric Data for PIV
• NIST 800-96 Cryptographic Algorithms
• NIST 800-116 (PACS Guidance)
• GSC-IS 2.3E

US FEDERAL GOVERNMENT CREDENTIAL SUPPORT
• CAC, CAC Transitional, CAC End Point
• PIV, TWIC, FRAC, PIV-I

LOGICAL & CARD READ PERFORMANCE
• T=0, T=1 Contact Smart Card Interface
• Type A and Type B Contactless Transmission Protocols
• Supports Collision Detection (Multiple Cards in Proximity) for both Type A and Type B
• Contactless Read Range: 95+% at 1.5 inches (3.8 cm)
• Maximum Read Range: less than 4 inches (10 cm)
• Supports Accelerated Transmission Bit Rates 106, 212 and 424 Kbits per second
• Default Wiegand format for FASC-N as defined in NIST 800-116 (Agency Code, System Code, Credential Number, Issue Code and Series Issue)

BIOMETRIC MODULE
• SECUGEN Biometric Module No. SDA-504
• Approved by FBI Std IQS, NIST 800-76 and FIPS-201

PHYSICAL
• High impact weather resistant polycarbonate with TFE Over-molding on Back Housing and Stainless Mounting Plate
• Dimensions: 9.50” high x 5.00” wide x 2.75” deep
• Smart Card Connector rated to 500,000 insertions
• Active LCD rated from -20F to +150F

USER I/O
• 2 Line by 16 character dot matrix active LCD display
• Red, Yellow & Green LED’s
• Audible Speaker

ENVIRONMENTAL
• Indoor or Outdoor.
• -25°F to + 150°F (-32°C to + 66°C)
• UL rain tested design
• 95% relative humidity (non-condensing)
• Weatherized shield recommended for outdoor installations

INSTALLATION
• Mounting Plate (included) with 4 screws appropriate for wall material.

SYSTEM INTEGRATION
• Cisco Systems
• Lenel/General Electric
• Quintron
• Honeywell/Vindicator
• AMAG/KABA/Hirsch/Galaxy
• Software House
• Schneider/TAC/Andover Controls
• Contact BridgePoint for Additional Integration Updates

ELECTRICAL
• Access System Input: Terminal Block or RJ-45 Connector
  Power: 12 Volt DC
• Access System Outputs: 48 bit to 200 bit Wiegand, RS 485, Mag Stripe.

WARRANTY
• 12 Months from Date of Purchase

TECHNICAL SUPPORT
• 866-562-5875; 08:00 to 17:00 Pacific Time M-F

ABOUT BRIDGEPOINT
BridgePoint secures facilities operated by the Federal Government and providers of critical infrastructure with trusted physical access solutions that are compliant with Federal security standards and guidelines. BridgePoint is a recognized technology leader with highly innovative solutions and our strong authentication technology is unprecedented in the security industry. Customers include the DoD, a number of government agencies and many large integrators. BridgePoint was recently selected as one of only two providers to demonstrate its trusted PACS solution as a GSA sponsored Federated PACS Demonstration Project. BridgePoint was founded in 1995 and is located in the San Francisco Bay Area. Information on BridgePoint can be found on the web at www.bridgepointsystems.com.