



Access Denied™ SYSTEMS

Bio ProximitySecurity System™ (KBPWS)

Automatically locks computer when user leaves, authenticates user upon return

Secugen



Wavetrend



The Bio ProximitySecurity System will:

- secure your data
 - provide a password replacement system
 - authenticate users
-
- Removes the "security responsibility" from irresponsible users.
 - Restores system to previously accessed screen when authorized user returns.
 - Identifies user by fingerprint, eliminating the need for passwords and cost associated with lost, stolen or changing passwords.
 - Provides multi-factor security to control threat of insider/employee data theft.
 - Assists with regulatory compliance, i.e., HIPAA, Sarbanes-Oxley Act, Gramm Leach Bliley Act.
 - Enhances customer confidence around securing personal and financial data.
- Compatible with the BeCrypt Encryption System.

Internal data security threats are no longer just an IT issue, but a business survival issue

The Bio ProximitySecurity System™ Contains:

(Model KBPWS)

- Bio Proximity Security System Software (on CD)
- Bio Proximity Security System Manual (on CD)
- Access Denied Systems - Wavetrend™ RF Receiver
- Access Denied Systems - Wavetrend™ RF Badge & Badge Clip
- Access Denied Systems - SecuGen™ Fingerprint Scanner

Technical Specifications

System Requirements

Operating System Requirements: Windows 2000 or XP
Ports: 1 USB Port, 1 RS-232 Serial Port (9 pin)
Disk Requirements: 15MB Free Space on C: Drive, CD Drive
Computer: IBM or Compatible
CPU: Pentium III or newer
RAM memory: 256 MB or greater

Base Receiver

Radio Frequency: 433 MHz
Bandwidth: ± 300 KHz
Sensitivity: -85 dB
PC Connection: USB Port
Range: 20 feet
Power: + 5Vdc (Via USB Port)
Physical Dimensions: 3.189" x 2.25" x .78" Oval Enclosure
Color: Ice Blue
Material: Fire resistant ABS
Weight: 72 grams
Certifications: FCC Certification, CE

Badge

Radio Frequency: 433 MHz
Physical Dimensions: 3.385" x 2.125" x .1968"
Clip: Vertical
Power: Internal long life lithium battery (3-5 year life)

Optical Scanner

Recognition rate: Less than 0.5sec
Resolution (dpi): 250
Effective Sensing Area: 12.9mm x 16.8mm 0.5" x 0.7"
Physical Dimensions: 27 x 40 x 73mm (1.1" x 1.6" x 2.9")
Weight: 100g (3.5 oz.)
Power supply (via USB port): DC 5V ±5%
Maximum power consumption: 100mA
PC Connection: USB Port
Operating Humidity: <90% relative, non-condensing
Fingerprint Technology: Optical (FDU04)
Data size (bytes): 2000 encrypted
FRR (False Rejection Ratio): 1/1,000
FAR (False Acceptance Ratio): 1/100,000
Overall Durability: Scratch and impact resistant (stress-tested to 40,000 psi), Rub-resistant to 10M rubs.
Certifications: U.S. GSA FIPS 201 APL, FBI Certification List for PIV

The Way It Works

The Bio ProximitySecurity System™ solves the access control problem by combining the best of two technologies: RF proximity and biometrics. The benefit of knowing when a user leaves the computer and the ability to absolutely, positively authenticate the user when they return is why this system surpasses even the most stringent password requirements.

In addition to the security aspect of the system, the cost savings with respect to password support, can run up to \$380 per user per year.

The Bio ProximitySecurity System™ is installed on the computer. The proximity distance is set for the computer (software settable by time, from 3 to 90 seconds). The Wavetrend™ Radio Frequency (RF) badges are assigned to the individual users. The users' fingerprint is scanned by the SecuGen™ fingerprint scanner. Minutia points are created, encrypted and stored on the computer with the users badge information.

Any attempt to deactivate the software by means of removing the Wavetrend™ RF receiver or SecuGen fingerprint scanner renders the computer inoperable (until the devices are reattached).

The system is locked when no active users are within the pre-selected proximity range. The keyboard and mouse cease to function and the monitor is blanked out.

As an authorized user approaches the computer, the computer senses the badge and verifies the badge is valid for this particular computer. The system requests the user authenticate themselves via the fingerprint scanner. The user is granted access to the system if the fingerprint matches the fingerprint assigned to that badge.

When the user leaves the proximity of the computer, the system automatically locks within seconds, regardless of any activity on the system (such as someone getting on the system and typing on the keyboard).

If a different authorized user approaches the computer and authenticates themselves, the computer will log the new user in as a new user. The previous user is then logged out. If the previous user returns to the computer without having anyone else accessing their system, they are returned to the screen they were on before they left the computer.

Since the system is automatically locked when an authorized user is not in the vicinity, the system is ideal for computers located in areas where non-authorized persons are located. The system is also ideal for the health care

Key Benefits

- Fingerprint authentication determines workstation access.
- Computer automatically locks as authorized user moves away.
- Eliminates the need for passwords.
- Ease of computer access results in high user acceptance.
- Compatible with the Mercury Enterprise Software system.
- Compatible with the BeCrypt Encryption system.



Access Denied
SYSTEMS

© ADS Inc. 2008 - All Right Reserved

Access Denied Systems, Inc.

10764 Indian Head Industrial Blvd.
St. Louis, Missouri 63132-1102
Phone: (314) 890-8566 Fax: (314) 890-9949
www.accessdeniedsystems.com