

# plusID™ universal biometric device

Be absolutely certain that the people accessing your facilities, networks and data are authorized to do so

Proof of identity is the key to security and access control. The **plusID** universal biometric fob uses a unique physical attribute – a fingerprint – to verify the identity of individuals seeking access to facilities and proprietary data. Using an on-device fingerprint sensor and secure storage and matching of the fingerprint template, **plusID** maintains privacy and is the ideal solution for rapidly and cost effectively enhancing both physical and IT security. **plusID**'s multiple wireless interfaces make it “out of the box” compatible with most installed security infrastructures.

## Advantages

1. The first mobile device to combine multiple security applications into one wireless biometric fob.
2. Fingerprint template and credentials are securely stored on the device, not in a central database – reduces the organization's risk and protects the user's privacy.
3. Verification everywhere it's required – can be quickly deployed without “ripping and replacing” existing physical security infrastructure.
4. Works with industry standard proximity, contactless smart card and one-time password systems, and stores credentials for physical and IT access, all in one device.
5. Low cost of acquisition, deployment, maintenance, and management.
6. Enables audit compliance by ensuring reliable authentication.

plusID front view



# plusID™ universal biometric device

## Product features

### One device for physical and logical access

- works in the same fashion as a standard prox card for physical facilities – doors and gates
- holds up to four contactless smart cards and four prox cards; supports multiple facilities and multiple card formats
- provides secure local and remote access to IT resources – such as applications, websites, VPN's, PCs, email, encrypted files
- uses advanced RF, Bluetooth™ and USB technologies\*
- supports one-time password implementations
- offers three-factor authentication

### Enhanced security with personal privacy

- secure on-device enrollment
- on-device fingerprint scanning, encoding and template matching
- biometric template stored in the device, not in a database
- transmits encrypted credentials, not biometric information
- secure ARM9-based processor
- designed to meet FIPS 140-2 level 3 tamper resistance

### Compatible with industry standards

- 125 kHz RF: works with HID®, Indala® and Kantech proximity systems
- 13.56 MHz RF: works with contactless smart card readers for doors, PCs and other systems; supports two-way encryption
- 2.45GHz Bluetooth™ wireless interface to computers and networks
- USB 2.0 for wired access

### Cost effective

- easy addition to existing physical security systems, no need to “rip and replace”
- works side-by-side with prox and contactless smart cards on the same card reader systems
- no need for a biometric database
- no need for biometric readers at each door and PC
- less than one second verification times
- two to three minute enrollment process
- can be erased and reissued

### Convenience

- key-fob sized device aggregates multiple access cards, fobs, and passwords
- personal biometric mobile devices upgrade security at every access point
- on-device fingerprint sensor means no single point of system failure and no congestion at doorways
- no health risks from shared biometric readers

\*Some capabilities are optional

## Technical specifications

### Certification

Designed to meet FIPS 140-2 level 3 tamper resistance.

### Hardware

**Microprocessor:** Broadcom BCM5890

**Memory:** 512K onboard flash available for template, credential, and application storage.

**Fingerprint Sensor:** AuthenTec 2510 with TruePrint® technology, 500 dpi swipe.

### Communication interfaces

125 kHz RFID

13.56 MHz (ISO 14443A, 14443B, 15693 and NFC (passive))

Bluetooth™ (2.45GHz)

USB 2.0 full-speed

### User interface

**Indicators:** green, yellow, red and blue LEDs indicate authentication requests, success and failure feedback, and Bluetooth™ connectivity.

**Buttons:** four multi-function push buttons; each configurable for the desired physical or logical application.

**LCD:** used for one-time-password display, personalization and low battery indication.

### Encryption

**Full Cryptographic Service Provider:** encryption and signature services are available on the device including key generation to support a PKI environment.

Encrypts data using AES-256 and RSA; hash using SHA-256. Utilizes x.509 certificates to ensure device authenticity.

### Battery

**Type:** Li-ion battery rechargeable using USB connection

**Battery Life:** : Average of 1,000 uses between recharges

### Physical

Length: 6.7 cm 2.6 in

Width: 3.6 cm 1.4 in

Depth: 1.2 cm 0.5 in

Weight: 24.1 grams 0.85 ounces

### Environment

**Operating temperature:**  
-20°C to +60°C; (-4°F to +140°F)

**Storage temperature:**  
-30°C to +80°C; (-22°F to +176°F)

**Operating humidity:**  
90% non-condensing

### Privaris U.S. issued patents

5,481,265, 5,729,220, 6,201,484, 6,441,770, D511,113, D511,114; additional patents pending.

Privaris Inc. focuses its technology expertise on the intersection of high security biometric applications and the individual's right to personal privacy. Privaris products authenticate the identity of an individual prior to that individual being granted access to facilities, resources, services, and transactions. Privaris Inc. is a privately-held Delaware corporation with its headquarters in Charlottesville, Virginia.

For more information:  
tel: 703.592.1180

# PRIVARIS®

[www.privaris.com](http://www.privaris.com)

plusID back view  
actual size

