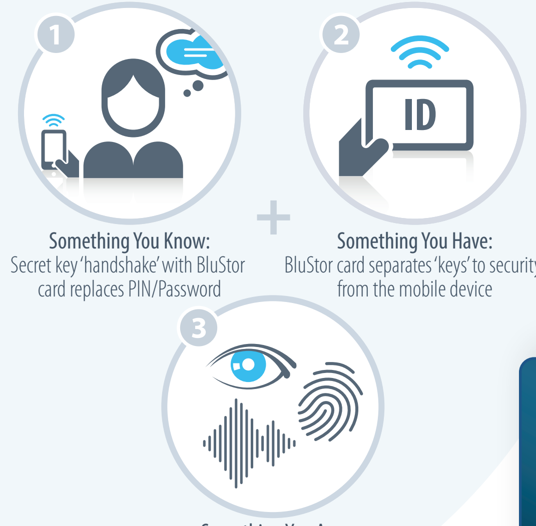
Why BluStor?

Because effective mobile security requires multi-factor, multi-biometric authentication



Something You Know:
Secret key 'handshake' with BluStor card replaces PIN/Password

Something You Have:
BluStor card separates 'keys' to security from the mobile device

Something You Are:
Multiple biometrics stored on BluStor card

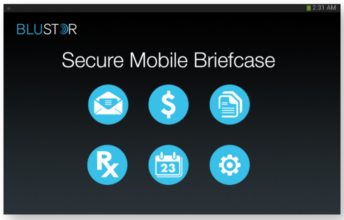
KEY FEATURES & BENEFITS:

- Biometric ID authentication using mobile device microphone, camera, fingerprint swipe, etc.
- Password vault: manage all passwords in one location
- Secure access to files and apps: email; web; bank/financial
- Bluetooth 4.0/LE; NFC; USB 2.0
- Ultra-thin rechargeable battery
- Secure digital wallet; store and manage multiple credit/debit cards
- Encrypted file storage with secure data backup to cloud
- 8GB flash memory
- Hardware cryptographic engine
- Compatible with iOS 7.0 or later, Android 4.3 or later

Introducing the World's First Multi-Factor, Multi-Biometric Bluetooth® Mobile Security Solution

Remote computing is transforming the way we work and play. But mobile computing brings increased risk of hacking and identity theft, and traditional 'single factor' security methods (PINs, passwords) are easily hacked. The BluStor system virtually eliminates hacking and identity theft by using hardware (a high-capactiy Bluetooth® card) and software (an iOS or Android app) to enable multi-factor, multi-biometric ID authentication — ideal for applications such as BYOD, health care, schools, or anyone seeking a secure mobile experience.

Using the BluStor Secure Mobile Briefcase app (SMB) a user can protect the entire mobile device or designate a 'secure' area on the device. To access the SMB the user provides a biometric, such as fingerprint, iris, or voice, and that input is compared with the user's biometric files stored on the BluStor card. Thanks to Bluetooth, the BluStor card can remain tucked away safely in a wallet or purse. If the BluStor card is not within range, or the offered biometric does not match the stored file, the SMB remains locked. And with 8GB of secure storage, the BluStor card has sufficient capacity for multiple biometric files and other data, such as email, work files, medical records, photos, music, and more.

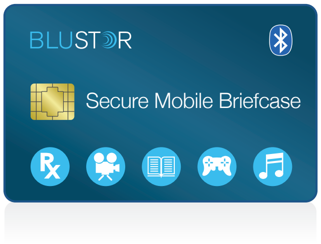

BLUSTOR
Secure Mobile Briefcase

In addition to biometric security, the BluStor SMB app comes with password vault, file encryption, and more. Users can add any app to the secure area simply by dragging it into the SMB folder.

Software

The SMB works with the BluStor smart card platform to create a complete mobile security solution, featuring:

- Biometric ID authentication using capture tools available on mobile device: microphone, camera, fingerprint swipe
- Password vault: manage all passwords in one location
- Secure access to apps: email; web; bank/financial
- Encrypted file storage
- Secure data backup to cloud
- Payment card management
- Requires iOS 7.0 or later, Android 4.3 or later



Hardware

The BluStor platform is the result of combining currently available technologies in a creative and proprietary solution:

- Dimensions same as those of a credit card
- Bluetooth 4.0 / BLE in dual mode
- High-performance and energy-efficient processor for smart cards
- 250MB – 8GB flash storage
- 7816-3 interface via a conventional serial reader
- Ultra-thin rechargeable lithium ion battery, with recharging mechanism via the USB/ISO 7816-3 interfaces
- Java Card OS (JCOP)
- Support for multi-factor authentication via on-card flash storage, a mobile phone/tablet, and a secure biometric authentication server
- Symmetric encryption of bulk data via the AES algorithm
- Hardware cryptographic engine to facilitate PKI-based applications, including asymmetric encryption and digital signature generation and verification
- Regulatory compliance for US, Europe, and other countries as required
- Optional fingerprint sensor
- Optional match-on-card verifications via fingerprints and iris

BLUSTOR

www.blustor.com