BLUSTOR
Powerful. Portable. Personal.

SOLUTION OVERVIEW

08 UNTETHERED NATIONAL IDENTITY & E-GOVERNMENT

With built-in Bluetooth 4.0 LE connectivity, BluStor can interface wirelessly with smartphones, tablets and laptops, securely transferring data 50 meters at rates more than twice as fast as NFC.

National Identity & eGovernment Services

Countries choose to implement a national ID card for a variety of reasons, including national security and law enforcement, employment, and easier access to government services. Countries that have embraced national identity cards, such as United Arab Emirates, India, and Malaysia, are at the forefront of this rapidly evolving technology. The UAE national ID card program is one of the most advanced, for the comprehensive security and functional features on the ID card, and the associated iris biometric project being deployed.

Biometrics—those unique personal characteristics: fingerprints, voice, iris, handprint—have been recognized as the only effective means to authenticate a person's identity. And multiple biometrics increase security exponentially. But due to limited storage on the smart cards now used (typically 28kB to 256kB), most existing national ID card systems can't handle multi-factor biometrics or the large data files that eGovernment applications of the near future will require. In addition, the need for bulky and expensive conventional or RFID card readers means today's ID card systems can't perform in an increasingly untethered mobile world.

For more information, contact Gregory Newman 949.233.7588 | gnewman@blustor.com

An 'Untethered' Mobile ID Authentication Solution

The BluStor Smart Card system enables the elimination of fraud while preventing identity theft in an untethered world, by providing answers to two simple questions: "Are you who you say you are?" and "Are you authorized to do this activity?"

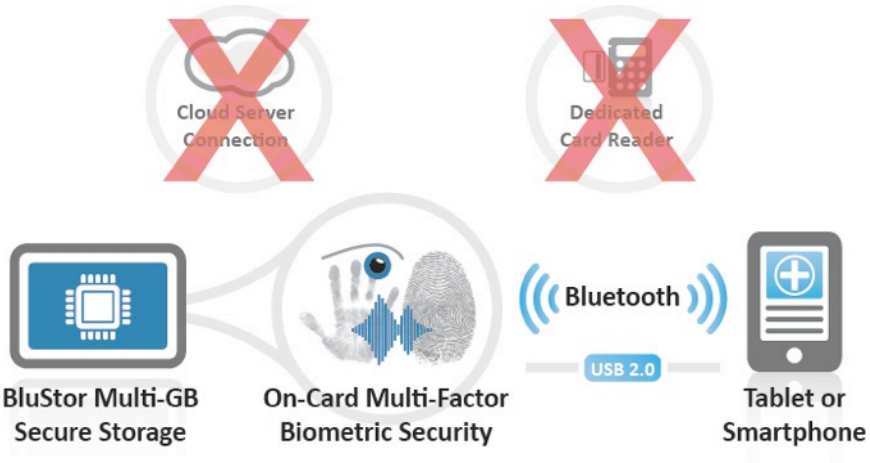
BluStor can provide this level of security because it offers biometric processing support, strong encryption capabilities, and sufficient storage capacity to allow for multi-factor biometric authentication without the need to connect to a central server.

Biometrics is the preferred method of user authentication, and will become ubiquitous as mobile devices add biometric reading capabilities. (Watch Walter Hamilton, Chairman International Biometrics & Identification Association, discuss biometrics and smart cards.)

Multi-biometric systems are now in use in large-scale U.S. government systems, including the Department of Defense, Department of Homeland Security, and Federal Bureau of Investigation. (Watch Tom Ridge, US Secretary Homeland Security 2003-05).

A 'Smarter' Smart Card Platform

With its unique combination of multi-factor biometrics, large storage capacity, and Bluetooth wireless connectivity, the BluStor smart card is the first solution that satisfies these demanding requirements. Based on breakthrough technology, the BluStor smart card platform enables effective, timely delivery of information in an untethered world, through multi-factor biometric identity authentication and secure high-capacity personal records storage—in a system that does not require an internet connection or a dedicated card reader. The BluStor solution is a flash-based storage device with robust encryption, a Bluetooth transceiver, and an energy-harvesting battery and recharging system—all in the form factor of a credit card that can be read by any Bluetooth-equipped smartphone or tablet.



Finis Conner (cofounder Seagate, founder Conner Peripherals) recognized the shift to 'untethered' computing, that today's smart cards are inadequate, and no alternatives exist to address this need. Hence BluStor: the smart card re-imagined: powerful, portable, personal.

The BluStor card provides the following comprehensive set of features:

- Multiple interfaces: Bluetooth 4.0 / Bluetooth low energy (BLE), NFC, USB, and ISO 7816-3. Bluetooth is available on virtually all laptops, tablets, and smart phones; the ISO 7816-3 interface supports legacy applications; and the USB interface is ideal for accessing bulk data, such as high resolution X-ray images.
- High capacity storage, 8GB and greater, for storing large amounts of data in multiple applications, including biometric data in a national ID card application, medical records and images in heath applications, and many other government applications.

Patented Technology

A U.S. patent has been issued for high-capacity smart card with a high-speed reader.

- *Patented High-Speed Smart Card with Flash Memory [US Patent 7,350,717 | Issued April 1, 2008]*

A patent has been filed for the unique combination of form factor, flash memory, energy-harvesting battery system and Bluetooth transceiver.

- *Bluetooth Enabled Credit Card with a Large Data Storage Volume [U.S. Utility Patent App. 13/418641 | March 13, 2012]*

With increasing storage and performance, new applications can be enabled. The smart card market is now at the stage that the hard disk drive market was at the introduction of the Seagate 5-1/4" 5MB HDD: the beginning of a major growth opportunity.

BluStor is positioned to drive this market, with patented technology and an executive team that has created and built some of the fastest-growing companies in history.

- Supports multi-factor biometric authentication, with optional match-on-card biometric verification.
- Physical security on the card, to prevent tampering.
- Ultra-thin, energy-harvesting polymer battery.
- Comprehensive cryptographic features, including symmetric data encryption and a PKI accelerator, to provide support for the four essential pillars of data security: privacy/confidentiality, authentication, integrity, and non-repudiation. These features enable many applications to have different types of data that are readable by users, but writeable only by authorized personnel.
- Provides storage to users as a mobile drive, for personal files.
- Supports document, computer, and network access control to:
  - Minimize loss of national security information, with encrypted and protected data.
  - Help minimize unauthorized leaks of data (e.g., WikiLeak) via extensive audit trails.
  - Help minimize security exposure via virus infection, when configured to be a read-only device by default. This helps prevent virus infection incidents like those that led to security exposures (via USB flash drives) at the U.S. Pentagon or at the Iranian Nuclear facility (StuxNet).
  - Ensure data that belongs to one application cannot be accessed by any other applications

BluStor meets all the requirements for a mobile, secure card platform for multiple high-end applications such as:

- National ID card/Driver's license
- Student ID card: attendance, library, lab, stored value
- Access control: facilities, computers, documents
- Housing: coupons, food stamps
- E-commerce: mobile payments, loyalty programs
- Medical: EMT, hospital, pharmacy, personal medical records

Existing applications can be migrated to the BluStor platform with minimal cost and impact, and upgraded as needed without replacing the card. Given its unparalleled security and storage capability, and that any Bluetooth-enabled mobile device can be a card reader, BluStor is the ideal platform for national ID cards and other eGovernment applications in a world where users increasingly access information via mobile devices.

For more information, contact Gregory Newman 949.233.7588 | gnewman@blustor.com