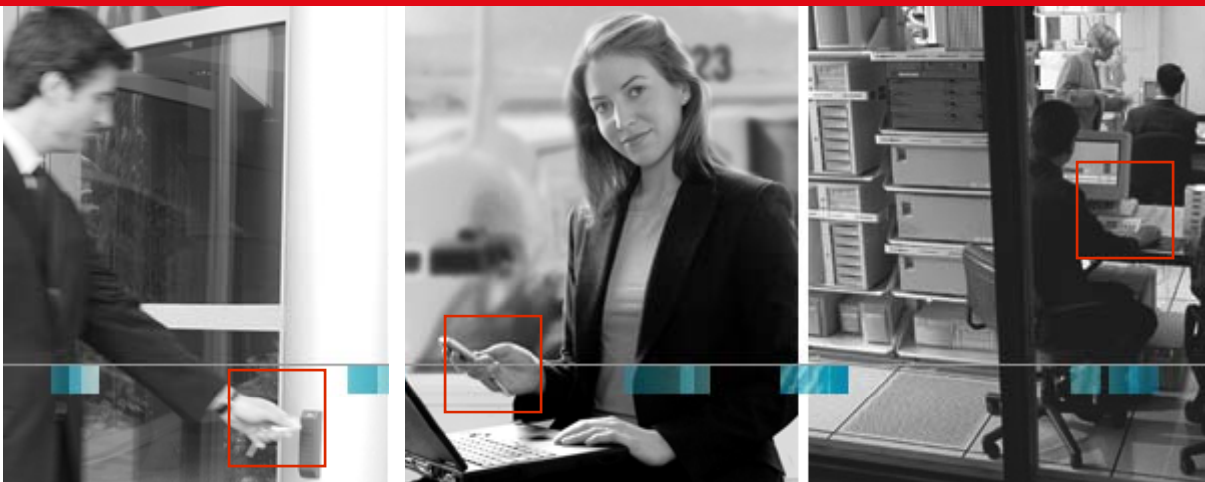


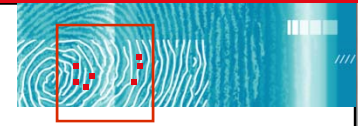
PRIVARIS®



Forget everything you thought you
knew about biometrics

A BIOMETRIC SOLUTION YOU CAN ACTUALLY SELL

Simple, secure, private

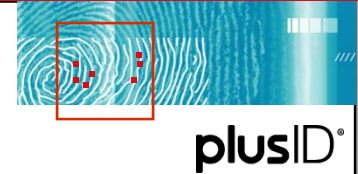


plusID®

Agenda

- Key drivers
- Identity verification
- Biometrics
- The ideal solution
- plusID overview

PRIVARIS®



Key drivers

- **Multi-factor authentication:** beyond access cards and passwords that can be lost, stolen or shared
- **Government compliance regulations:** HSPD-12, FFIEC, SOX, PIV, HIPAA...
- **Costly solutions:** inability to take advantage of legacy security infrastructure
- **Complex solutions:** user frustration results in workarounds and security gaps
- **Convergence:** consolidation of logical (IT) and physical access devices and methods
- **Increasing privacy concerns:** databases with personal information continue to be compromised

PRIVARIS



Identity verification

■ The real need

- knowing exactly who is at the door or keyboard – the security industry's ultimate goal – before granting access

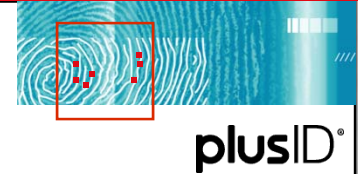


■ The challenge

- reliably verifying identity *without* excessive expense, complexity, or invasion of privacy
- leveraging investments in existing security systems



PRIVARIS



Biometrics. A logical approach to identity verification

- **Something you “are” – identifies users based on an innate biological characteristic**
 - as opposed to something you “have”
 - or something you “know”
- **Meets audit requirements**
 - can’t be lost, stolen or shared
 - offers multiple authentication factors
- **Convenient**
 - no passwords to remember
 - no access cards to carry

PRIVARIS®



Biometrics. What comes to mind?

- **Costly and complicated**
 - requires ripping and replacing existing security infrastructure
 - requires installation of new biometric readers at every door
 - disruptive to business operations
 - risk and liability of storing/protecting users' biometric data
- **Common/shared biometric readers**
 - single purpose – support only physical access
 - long lines during high traffic
 - health and hygiene issues
- **User concerns**
 - difficult to use, inconvenient, invasive
 - privacy concerns over relinquishing personal biometric data

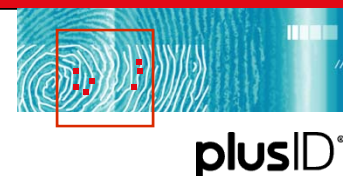
PRIVARIS®

What if.....?

Imagine the benefits of biometric identity verification without the traditional drawbacks

- **What if biometrics could be:**
 - **deployed overnight** – no costly or complicated installation
 - **easy to use** – non invasive, reliable and convenient
 - **private** – no need to collect or protect personal biometric data

More organizations would use biometrics to solve the identity verification challenge

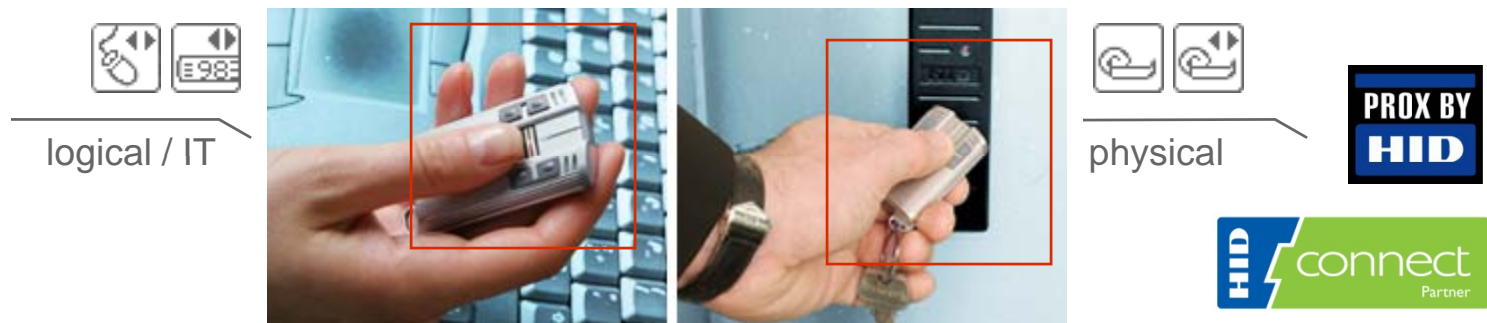


PRIVARIS®

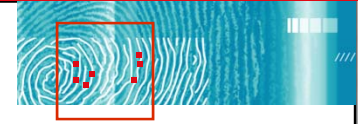


plusID – the solution

- The **world's first** wireless personal biometric device
 - Verifies identity via fingerprint *before* releasing **standard credentials**
 - **Compatible** with existing security systems – *no installation required*
 - **One device** for both physical and logical access – *convergence*
 - Accurate **verification** of user's identity – *regulatory compliance*
 - Ensures and protects user's **personal privacy**



PRIVARIS®



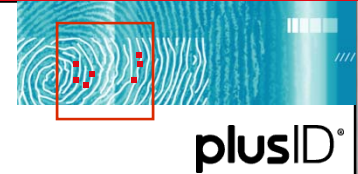
plusID®

How plusID works



- 1 Push a button to select the access point (door, gate, computer, etc.)
- 2 Scan finger
- 3 Device compares scanned finger to stored template - a positive match releases the appropriate access code, biometric never leaves the device
- 4 Access is granted

PRIVARIS®



How is privacy assured?

Other fingerprint-based security systems

- Use a biometric database with associated risk and liability
- Require transmission of fingerprint
- Have readers and/or a database that can be compromised

Privaris plusID

- Secure enrollment software
- Biometric template enrolled into the secure token (*never* transmitted, *no* central database)
- First use of Broadcom's new BCM5890 secure processor
- Device conforms to FIPS 140-2 level 3
- A cryptographic service provider - transmits encrypted credentials, *never* biometric information
- Useless if lost or stolen

PRIVARIS



How are compatibility and convergence achieved?

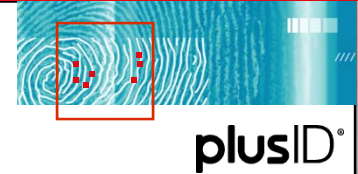
Compatible with industry standards

- **125kHz** proximity card - common door readers
- **13.56MHz RFID** contactless smart card readers - doors and computers (ISO14443A/B, 15693 & NFC)
- **ISO 7816** - device presents itself as a smart card to operating system
- **USB** for “tethered access,” to computers and networks
- **2.45GHz Bluetooth™** to access computers and networks
- **One-time-password** delivery for remote access to computers and networks

Compatible with existing systems

- **Works** with existing access control infrastructure -HID, Indala and CASI door readers
- **Compatible** with Microsoft® native smart card infrastructure for logon
- **No complex installation** – non-disruptive, no middleware, wiring or coding required, and no database. Simple two-minute enrollment process
- **Low cost** of acquisition, installation, deployment and maintenance - devices are reclaimable and reusable, password maintenance costs are reduced

PRIVARIS®



How does **plusID** compare to most biometric solutions?

“Centralized” solutions with fixed biometric readers/sensors

- Require biometric readers at every door, every PC
- Single point of failure = traffic congestion at access points
- Require collection and protection of biometric data
- Require hard wiring into a network, network equipment
- User still requires multiple access devices (prox cards, fobs, password generators)
- An all or nothing proposition

Privaris **plusID**

- Affordable personal biometric readers on every user’s keychain – not at every door or PC
- “Distributed” solution means no single point of failure and no traffic congestion at doorways
- No biometric database required
- Upgrades security levels at all access points – not just ones with biometric readers
- Enables convergence of multiple physical and logical access devices
- Enables a partial biometric deployment for select employees/areas

PRIVARIS



A practical solution to the identity verification challenge

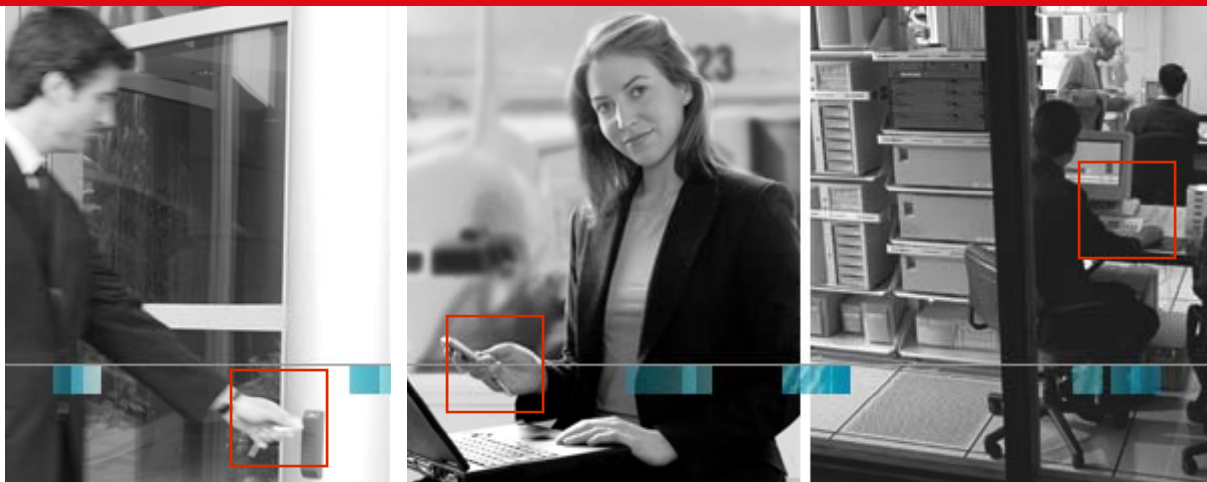
- Enhances security with no impact on existing systems
- A unified identity solution for physical *and* logical access
- Enables rapid, affordable and streamlined implementation
- Reduces complexity for organizations and users



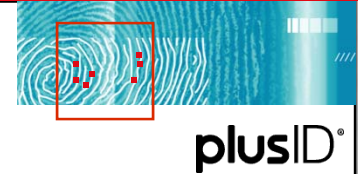
Secure, simple, private.

PRIVARIS

PRIVARIS®



plusID Manager Enrollment Software overview and demonstration



Products

- **plusID 75:** a version of the plusID that includes Bluetooth and the RSA SecurID one-time password for remote logon
- **plusID 90:** a long-range version of plusID that opens gates from within a closed vehicle at speed
- **bioBase:** a government Personal Identity Verification (PIV) biometric smart card holder that enables agencies to meet pending government authentication requirements (FIPS 201/HSPD-12) for physical and logical access related to homeland security
- A **financial** version of the plusID for biometrically authenticated credit card payments, in-lane or online

PRIVARIS



About Privaris

HISTORY

Founded in 2001

First product in March 2004

plusID launched July 2007

FUNDING

Private investors

Oct 2005: Harbert Venture Partners, Noro-Moseley Partners, River Cities Capital Funds, RedShift Ventures

MANAGEMENT

John Petze, President & CEO

Barry Johnson, Co-founder, CTO

Mike Kohonoski, COO

Steve McDorman, VP Sales

FOCUS

Developing and integrating technology to create new products in the area of biometric security while maintaining the privacy of the individual

MAJOR PARTNERSHIPS

HID®, Broadcom, RSA

HEADQUARTERS

650 Peter Jefferson Parkway

Suite 330

Charlottesville, VA 22911

www.privaris.com

PRIVARIS®