



**PRIVARIS®**

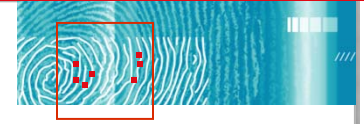
*The Identity Verification Challenge*

Too Many Passwords and Cards?

It's Time for a Unified Approach to  
Identity Credentials

**John Petze, President & CEO Privaris, Inc.**

**Financial Services  
Technology  
Forum**  
**October 2007  
Toronto  
Ontario**



2

# Identity verification

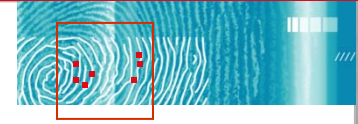
- **The real need**
  - knowing exactly who is at the door or keyboard before granting access and privileges
  - verification of identity is fundamental to almost all security applications
  
- **The challenge**
  - reliably verifying identity *without* excessive expense, complexity, or invasion of privacy
  - leveraging investments in *existing* systems



**PRIVARIS®**

# Business Drivers – Risk and Cost

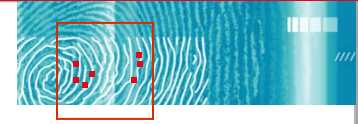
- **Societal need for heightened security**
  - to physical resources – buildings and facilities
  - to IT resources – computers, networks, applications
  - for financial transactions
- **Regulatory compliance** demands non-repudiable audit trails
- **Costs and complexity** associated with current approaches – numerous passwords, credentials and tokens
- **Creating a security environment that works** – avoid burdensome security requirements
- **Convergence**



3



**PRIVARIS®**



4

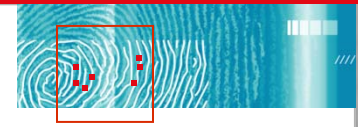
# Traditional approaches

(My Rule of Too's)

- **Passwords and Access Cards**
  - Two different things
    - passwords don't get you in the door
    - cards don't get you on the network
  - Too easily shared, lost, or stolen
  - Too complex and too many – we write them down!
  - Too expensive
    - password support costs -- \$150 - \$300 per year/per employee (Gartner)
  - Too weak in verification – don't prove identity



**PRIVARIS**



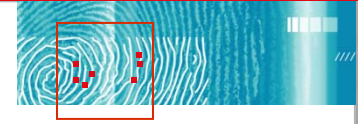
5

# Cards for physical access

- Individual access cards and fobs for separate buildings & facilities
- Enable “buddy punching”
- Useable if lost or stolen
- Separate issuance and management process from logical access credentials



**PRIVARIS®**



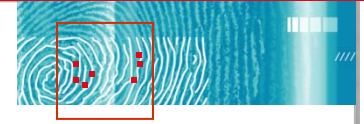
6

## And then there are biometrics...

- **Accuracy**
  - offers reliable identity verification
  - can't be lost or stolen or shared
  - non-repudiable – supports audit requirements
- **Based on something you “are” as opposed to:**
  - something you “possess” (access card)
  - something you “know” (PIN or password)
- **Convenience**
  - no passwords to remember
  - no need to carry multiple cards/keys
- **BUT...**



**PRIVARIS®**

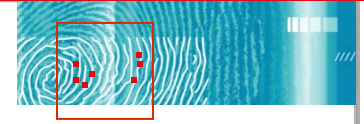


7

# Biometrics – What comes to mind?

- **“Screwing stuff to a wall”**
  - expensive and disruptive
  - new readers at *every* door (or gate or PC)
  - running power and network wiring
  - single purpose – supports only physical *or* logical access
- **Invasive**
  - users relinquish sensitive biometric data to a 3<sup>rd</sup> party for “safe keeping”
  - user distrust

**PRIVARIS®**



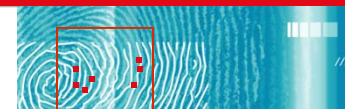
8

# Biometrics – What comes to mind?

- **Shared biometric readers**
  - health & hygiene issues
  - long queues during high traffic periods = reduced productivity, user frustration
  - single point of failure = extreme consequences
- **New Risks**
  - Enterprise liability for storing and protecting sensitive biometric data
  - a “new” potential target for hackers

**PRIVARIS®**

# What if....?



9

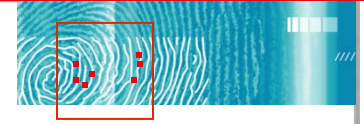
You could have the benefits of biometric identity verification without the traditional drawbacks

- **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 applications would use biometrics to solve the identity verification challenge*

**PRIVARIS®**



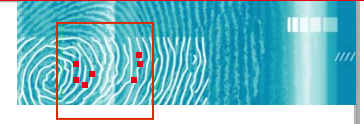
10

# Time for a new approach

- *We need to implement biometric identity verification in an entirely new way...*
- Biometrics can be personal and private
- A safe and easy way to “prove its you”



**PRIVARIS®**



# Personal Biometrics

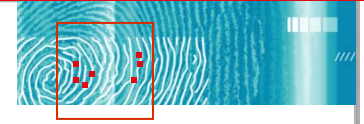
- **Biometric identity verification in your hand – not on the wall**
- **A personal wireless token with built-in fingerprint reader**
- **Verifies identity** via fingerprint before releasing credentials for:
  - computers, networks & applications (**logical access**)
  - financial transactions (**in-lane and on-line**)
  - doors & vehicle gates (**physical access**)



logical access



physical access

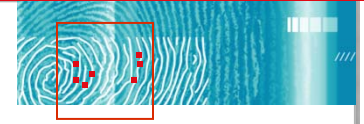


12

## A new approach...

- **No new equipment to install or wire**
  - works with existing systems – contactless payment, physical and logical/IT security systems
- **Multi-function**
  - a single token replaces both access cards, passwords, contactless credits cards
- **No biometric database required**
  - all fingerprint processing and matching done on secure, personal device – fingerprint never leaves device

**PRIVARIS®**



# How personal biometrics work



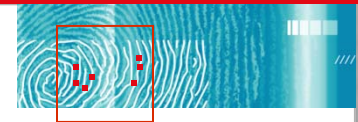
- 1 Push a button to select the mode (credit card, door, computer, etc.)
- 2 Scan finger
- 3 Device compares live finger to template stored in secure memory - a positive match releases the appropriate credential code
- 4 Existing system determines if access granted or transaction approved

That's it.

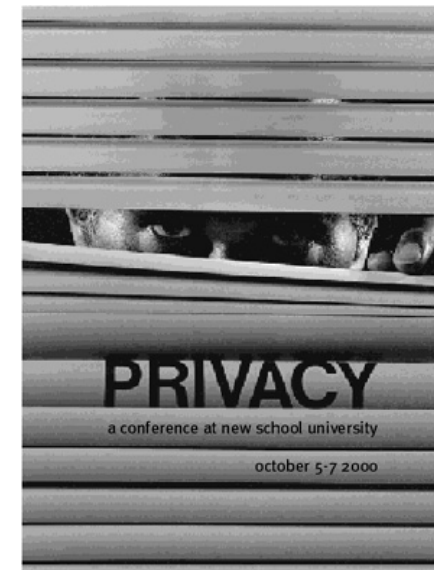
**PRIVARIS®**

# Addressing personal privacy

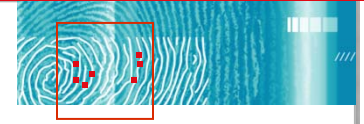
- **The user remains in full and exclusive possession of their biometric data**
  - never shared, collected or stored in any external system
  - never transferred – this approach separates identity verification from credential delivery for a more effective model
  - stored in encrypted memory on their personal device
  - un-sniffable – only transmits when activated by rightful owner



14



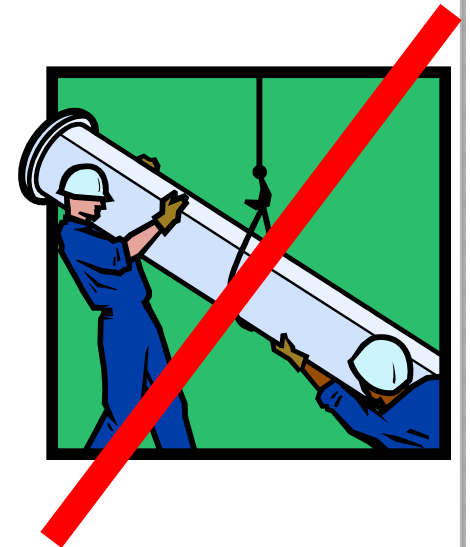
**PRIVARIS®**



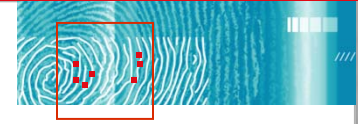
15

# Non-disruptive

- **Enables rapid, affordable implementation**
  - no “rip and replace” of existing hardware
  - works with what’s already in place
  - no middleware, wiring, or coding required
- **Outputs signals compatible with existing infrastructure:**
  - proximity card readers (at doors)
  - contact & contactless smart card readers (at doors, computers, point of sale)
  - one-time passwords

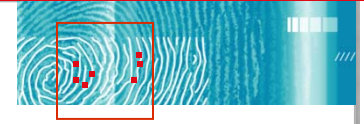


**PRIVARIS®**



# Universal compatibility

- **Working with accepted industry standard technologies:**
  - **13.56MHz RFID** contactless smart card readers - doors and computers (ISO14443A/B, 15693 & **NFC**)
  - **125kHz RFID** proximity - common door readers
  - **ISO 7816** – plusID presents itself as a **smart card** to a PC – Windows operating system for logon
  - **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



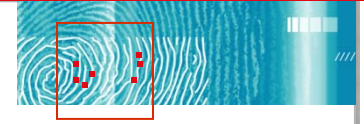
17

## Convenience and simplicity

- A single secure token for both physical, logical, & financial
- Eliminates need for multiple access cards and passwords
- Fast and easy to use - verification times of a second or less
- Personal, portable verification = no traffic back-ups



**PRIVARIS®**



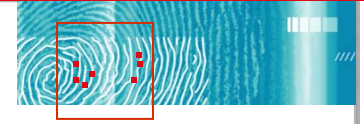
18

## Reduced liability

- Eliminates risk and expense of collecting and protecting employee/customer biometric data
- User's enroll in their personal device – not a database
- Fingerprint templates securely stored and matched on the device, never transmitted
- No privacy issues to manage – easier on the HR department and consumer public



**PRIVARIS**



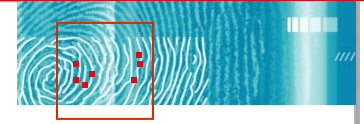
19

# Addressing the hygiene issue

- No need to touch a public biometric reader that's shared by all – especially during cold and flu season
- Reduces bio-terrorism concerns



**PRIVARIS®**



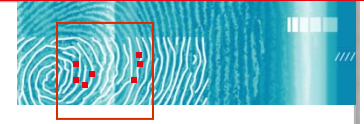
20

## Plays well with “single sign-on” in the enterprise

- Single Sign-On (SSO) software is a new trend to simplify the password challenge, particularly in corporate environments where they must be frequently changed
- Users log into the SSO package with a single username/password
- SSO package takes over the responsibility for logging into the additional applications

***But with the convenience of SSO comes a new risk...***

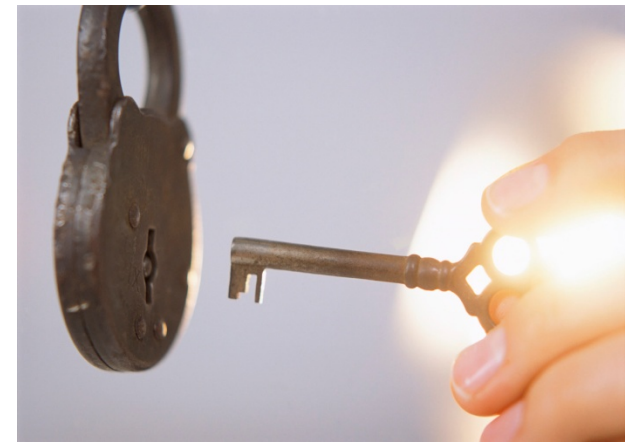
**PRIVARIS®**



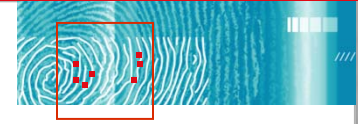
21

## With SSO a new risk

- Before SSO, gaining access to one of a user's many passwords gave access to a small part of their life and data
- Now one password is the key to the entire kingdom...
- *SSO brings with it the need for a more secure form of identity verification*



**PRIVARIS®**



22

# Enabling Convergence

- **A unified credential solution**
  - addresses need for **strong authentication**
  - credentials *only* delivered after a **biometric verification** of identity
  - streamlines **identity management** while enhancing security
  - securely carries and delivers a **variety of credentials** compatible with existing infrastructure
  - **converges** the identity credential across the boundaries physical, logical and financial transaction



*Crosses the boundaries between the different domains – physical, logical & financial*

**PRIVARIS®**