



## **Managing Identity Security for Compliance and Business Efficiency**

*Achieving compliance certainty that is user convenient*

**A DigitalPersona White Paper**

September, 2008

DigitalPersona, Inc.  
650.474.4000  
[www.digitalpersona.com](http://www.digitalpersona.com)

© DigitalPersona, Inc., 2008

## Table of Contents

Introduction.....	1
The Identity Security Challenge .....	1
Identity Security Control Solutions .....	4
Solution Alternatives.....	2
A Breakthrough - Fingerprints .....	3
Required Today: Strong Passwords .....	5
Required Today: Secure Communications .....	6
Required Tomorrow: Multi-factor Authentication.....	7
Required Tomorrow: Transaction Proof of Presence.....	8
How DigitalPersona's Identity Security Technology Works .....	9
Summary .....	10

---

## Introduction

With nearly every facet of enterprise operations now dependent on or supported by IT systems, the stakes involved in identity-related security risk have risen dramatically in recent years. Business risks ranging from minor policy and compliance violations to major business losses occur every day. All it takes is a single person with the wrong privileges and intent.

### Identity security risk is critical:

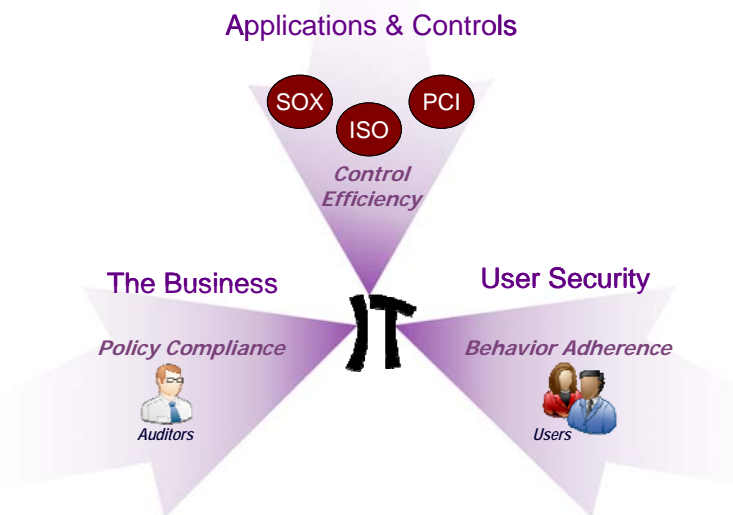
- The #1 cause of compliance deficiencies is lack of user and application access controls.  
*IT Policy Compliance Group Report, July 2007*
- 71% of enterprises believe identity compliance activities are strategic – rated as important or very important.  
*Ponemon Institute Survey Results, August 2007*

But how much investment in identity security is enough today? And what about tomorrow? This white paper addresses these questions for IT practitioners who need to satisfy auditors and users, as well as their employers.

## The Identity Security Challenge

Every IT organization walks a fine line at the intersection of application security controls, user needs and auditor scrutiny. Security control requirements vary from one regulation to the next. Users always want faster access. Auditors have their own opinion as to what's effective.

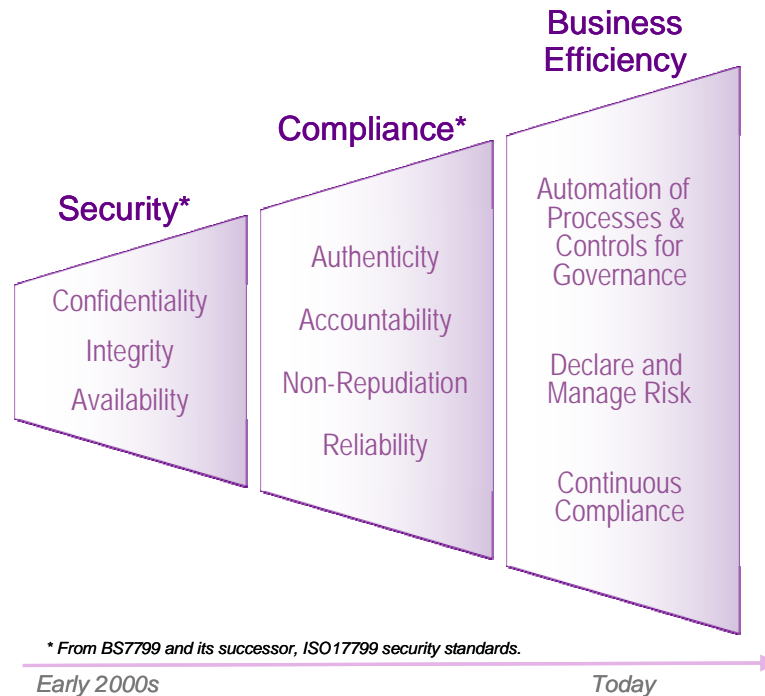
### Identity Security Requirements Are Squeezing IT



Standards like ISO17799 provide IT organizations with guidance. However, these standards are evolving rapidly to keep pace with the ever-changing nature of IT systems and user behaviors.

In 2005, the ISO17799 standard added authenticity, accountability, non-repudiation and reliability requirements to provide more granular audit information, as shown below. Today, auditors are moving organizations toward proactive risk management. They want the business to “prove innocence” *before* anything bad happens.

## Identity Security's Evolving Requirements



PCI, for example, is driving organizations to be liable for breaches as of the time a breach occurs, not as of the last audit. SOX audits under the new “Audit Standard 5” rule encourage businesses to proactively “self assess” and manage their business risks.

To survive, organizations must find ways to formally integrate compliance into the business. This usually requires automating identity security controls to pay for the investment. And they must demonstrate that automation works continuously, all the way down to the user-activity level.

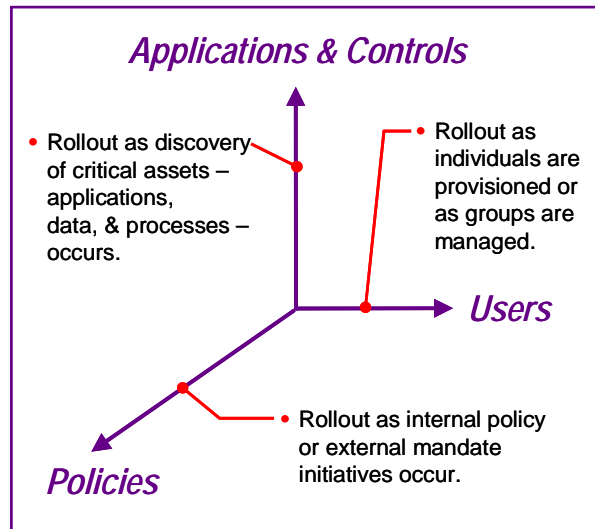
## Solution Alternatives

All identity security controls address the same fundamental needs. The organization needs to know the identity of who performs an action and their “intent” such as authorizing a transaction, viewing personal information, manipulating financial data, and so on. Because identity security controls directly impact users, they can increase security, compliance and business efficiency, *only if* they are deployed by IT in ways users embrace.

Perhaps the most important aspect of rolling out identity security controls is “incremental deployment” due to:

- Requirements for identity security controls occur in waves as regulations mature and policies get defined.
- Controls typically require deployment against specific networks, applications and users, as discovery of sensitive information occurs.

Inability to satisfy incremental control deployment can be the difference between viability and impracticality of an automated solution.



In addition to rolling out policies at various times and for various users and applications, IT also needs to vary the control strength – from strong passwords, to encrypted communications or multi-factor authentication – depending on the use and nature of the target application or resource to be protected.

Most identity security controls including strong passwords, tokens, single sign-on, and other solutions have the following problems:

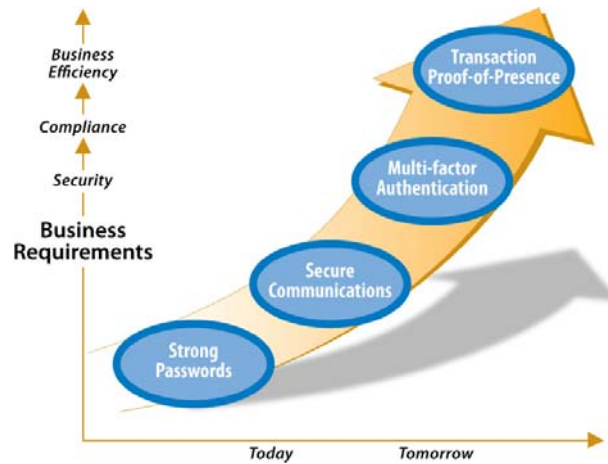
- **Can't be deployed incrementally** – most solutions don't allow IT to add users and applications as needed. Typically, policies need to be strengthened over time by applying different controls to various users and applications.
- **Don't ensure individual accountability and compliance** – passwords, tokens and cards can be lost, stolen or shared, limiting their effectiveness in identifying user actions.
- **Are too slow or bulky for individual transactions** – products that are time-consuming or physically inconvenient deter usage, making them impractical for securing low-level transactions.
- **Force choice of security over convenience** – passwords that are strong enough to be secure get written on "sticky notes" while cards and tokens have to be kept accessible.
- **Drive up operational costs** – help desks get burdened by password resets, token or card inventorying and re-provisioning.

## A Breakthrough: Fingerprints

The four fundamental identity security controls required today or in the very near future include strong passwords, secure communications, multi-factor authentication, and transactional proof-of-presence. The good news is that implementing identity security controls can satisfy auditors, users and the business simultaneously. The question is: how can they be implemented effectively?

Unlike other identity security controls, fingerprints are based on a physical characteristic: who you are, not what you know. Users simply touch their finger to a reader and are immediately authorized and logged into the network, application or Web site.

As a result, millions of fingerprint readers are now embedded as standard equipment on most laptops shipped today or they are easily added to existing PCs using peripherals. IT is now able to centrally manage widely-distributed fingerprint sensors as a natural interface for the four major identity security controls.



Identity Security Control	Definition	Fingerprint Breakthrough
<b>Strong Passwords</b>	Difficult to detect by both people and software, passwords must consist of at least six characters incorporating a combination of letters, numbers and symbols.	Users no longer have to care how complicated passwords are or how often they're changed.
<b>Secure Communications</b>	Encrypted and digitally signed instant messages, email and electronic documents protect data in motion and workflow transactions.	Users can digitally sign and encrypt instant messages, email and Office documents with the touch of a finger in place of entering a password.
<b>Multi-factor Authentication</b>	Irrefutably links individuals to log-on by requiring "something you have" and "something you know".	User fingerprints replace tokens, relieving IT of token distribution and management burdens.
<b>Transactional Proof-of-Presence</b>	Extends security by confirming identity in recurring purchases, trades or authorizations. Required for continuous compliance and fraud reduction.	IT and the business can sustain investment in security by paying for it with decreased IT burden and help desk calls, and increased worker productivity.

Fingerprint identity security solution effectiveness comes from simultaneously meeting the needs of auditors, users and the business with:

- **Compliance Certainty** – Fingerprints allow auditors to know who accessed what resource and when by linking users to their actions.
- **Security Simplicity** – Users embrace fingerprints as a far easier means of authenticating themselves over passwords and tokens.
- **Business Efficiency** – IT and the business can sustain investment in security by paying for it with decreased IT burden and helpdesk calls, and increased worker productivity.

## The Four Identity Security Controls in Action

### Required Today: Strong Passwords

Passwords are the most pervasive mechanism used to secure access to networks and databases. Unfortunately, password authentication is often the weakest link in the security infrastructure. Not surprisingly, most auditors, regulators and industry best practices require use of strong passwords.

The absence of strong password use can increase the liability organizations face when a breach occurs. Court interpretation of “due care” in corporate governance, and therefore liability, is often determined specifically based on use of industry best practices.

### Security and Strong Passwords

Despite countless hours spent creating policies, designing procedures and purchasing safeguards, a single user can undo all of IT’s efforts by simply sharing a password, even a strong one. Users aren’t perfect and typically are more concerned with getting their jobs done than in following policies.

Two-thirds of workers polled in downtown San Francisco turned over their passwords without hesitation when asked. Their reward: a coffee coupon for \$3. Of those who said “no way” to the request, 70% still gave up hints, like anniversary date, wife’s or pet name.

*Bank Information Security, April, 2004*

Strong passwords, centrally managed by IT, take the burden of managing passwords away from users. Fingerprints used to access networks, operating systems and applications still utilize a strong password credential providing compatibility with existing infrastructure. That credential can even be made invisible to the user.

### Compliance and Strong Passwords

Most regulations and mandates<sup>1</sup> require use of strong passwords to ensure the confidentiality and integrity of information. For example:

**SOX** – from general audit guidelines: requires that fundamental security requirements be addressed, including confidentiality of financial records to ensure no one except financial officers, auditors, and executives have access to the data.

**PCI** – from the mandate: “Assign a unique ID to each person with computer access – using strong passwords.”

**HIPAA** – from the legislation: Technical Safeguards include: “Limit access to personal health information (PHI) to employees who have a business need to see it” and “store electronic PHI on a secure server accessible only with a password or other control.”

**GLBA** – from the legislation: Physical Safeguards include: “Use password activated screensavers; Use strong passwords that change periodically; prevent passwords from being written down.”

**NERC-CIP** – from the mandate: CIP-003 Security Management Controls, “End user account management including strong passwords; manage factory default accounts including removal, disabling or renaming accounts.”

**ISO17799** – from the standard: “Section 9.2.3: Establish a password management process; Section 9.3.1: Encourage users to protect passwords; Section 9.5.4: Set up a good password management system.”

---

<sup>1</sup> Formal regulation names listed in end note.

## Business Efficiencies and Strong Passwords

Paying for strong passwords is easy if the solution isolates users from the process of managing their passwords. Centrally managed strong passwords eliminate helpdesk calls, an easily quantifiable savings for most organizations.

### Support Cost Savings Metrics

- Between 25 to 40% of all help desk calls are for password problems. *Forrester*
- Average cost of a password reset call is between \$10 and \$31. *Forrester*
- Each year companies spend up to \$150 per user trying to maintain secure passwords. *Gartner*

In many cases, eliminating password resets also results in:

- Desktop productivity improvement from fewer delays accessing corporate applications
- Point-of-service quality improvement from faster time to the information needed by call center or other customer-facing users.

For example, in Citicorp's call center, employees use fingerprints to quickly access information for improved service levels. Previously, each forgotten password seriously impacted banking workflow. Using fingerprints, workers now access multiple databases and accounts, all of which use different, frequently changing passwords.

## Required Today: Secure Communications

Compliance with regulations and mandates does not ensure security. In March of 2008, as a result of computer systems being "illegally accessed during transmission of card authorization," Maine-based Hannaford Brothers grocery chain announced that 4.2 million customer card transactions were compromised. More than 1,800 of those credit card numbers had already been used for fraudulent transactions. Within two days of the breach announcement, customers filed two class action lawsuits against the retailer. Despite being PCI-certified in February of 2008, the suits charge Hannaford was negligent for failing to provide adequate security for computer data.<sup>2</sup>

Data in motion is particularly difficult to protect given the cost and complexity of implementing encryption for most organizations. However, according to a Network World article as early as January of 2007, corporate-wide encryption is listed as one of seven best practices.

**Best Practice #5:** Look at all aspects of electronic communication and data manipulation throughout your enterprise. That should include all instant messaging, file transfer, chat, e-mail, online meetings and webinars, plus all data creation, change, storage, deletion and retrieval.

*Gary S. Miliefsky, Network World, January 2007*

---

<sup>2</sup> [www.bankinfosecurity.com](http://www.bankinfosecurity.com), April 4, 2008

## Security and Secure Communications

Fortunately, identity-based secure communications provides organizations with effective means for protecting against external threats and loss prevention due to insider abuse. Because traffic is encrypted from the user device to its destination, the ability to compromise transmissions externally is eliminated.

Furthermore, because user identities are tied to transmissions, user awareness of the control itself becomes a deterrent to improper handling of sensitive information. This includes transmission of information using email, instant messaging, files, approval authorizations and other communications.

## Compliance and Secure Communications

Establishing audit trails for communications using electronic signatures is called out by many major regulations and mandates including PCI, HIPAA, GLBA, FDA 21CFR11, as well as being a long-time requirement among security standards such as ISO17799. For example:

**PCI** – from the mandate: “Encrypt cardholder and sensitive information across public networks – using digital signatures for transaction approvals.”

**HIPAA** – from the legislation: “Transmission Security, 164.312(e)(1), Integrity Controls, Encryption.”

**GLBA** – from the legislation: “Technical Safeguards include “Encrypt sensitive customer information transmitted electronically.”

**FDA21CFR11** – from the regulation: recommends use of “Electronic signatures that are intended to be the equivalent of handwritten signatures, initials, and other general signings required by predicate rules. Part 11 signatures include electronic signatures that are used, for example, to document the fact that certain events or actions occurred in accordance with the predicate rule (e.g., approved, reviewed, and verified).”

## Business Efficiencies and Secure Communications

Business efficiencies resulting from secure communications result from two primary sources:

- Automating business process that would otherwise not be possible due to security concerns
- Improved worker productivity for processes where identity security controls must be implemented for compliance or internal governance purposes.

Automation using email and sensitive document transfer between lawyers, doctors, financial advisors and their clients save time and money given the high value work performed. Automating the many processes involving personal or credit card information also saves time and money by eliminating paper document storage and associated handling and retrieval costs.

Where electronic documents can be signed and electronically backed by the non-repudiation provided by digital certificates, further savings result from the reduced time to compliance during audits.

## Required Tomorrow: Multi-factor Authentication

Because multi-factor authentication has been in use for some time using tokens and smart cards, particularly for remote access to corporate systems, auditors are increasingly interested in promoting it where feasible due to its effectiveness in associating individuals with their activities.

## Security and Multi-factor Authentication

Multi-factor authentication is most commonly used to safeguard remote access. However, its security effectiveness and new desktop operating system security features has auditors pushing multi-factor authentication to the desktop as well. The feasibility of implementing multi-factor authentication has always been the challenge given the requirement for users to carry a token, smart card, or something else “they have” in addition to using a password, pin or “something they know”. Eliminating the need to carry a token or smart card by replacing it with fingerprints provides an economic basis for even small to mid-sized organizations to afford this advanced level of identity authentication.

## Compliance and Multi-factor Authentication

While multi-factor authentication may not be required for every organization today, it is emerging quickly as a viable control option by auditors, primarily due to the maturity of alternative technologies available and the more affordable, economics mentioned above.

For example, several key mandates and regulations specifically call for use of multi-factor authentication as follows:

**PCI** – from the mandate: “Protect stored data – using multi-factor authentication to data at rest; restrict data access to need-to-know – using multi-factor authentication to data at rest: restrict physical access to cardholder data – using multi-factor authentication.”

**SB1386** – from general audit guidelines: “Ensure confidentiality of personal data; no one except designated employees to have access to the data without using strong authentication. Ensure no tampering of personal information using strong authentication and non-repudiation for access to stored data.”

**NERC-CIP** – from the mandate: “CIP-005 Electronic Security, “Implement strong measures to ensure authenticity of the accessing party. These strong procedural or technical measures shall include at least one of the following measures: Two-factor authentication or digital certificates.”

**ISO17799** – from the standard: “Section 9.4.3: Use cryptographic methods to authenticate remote users using strong protection; Section 9.5: Restrict Access at OS Level; Section 9.5.3: Identify and authenticate all users: optionally use biometric authentication technologies.”

## Business Efficiencies and Multi-factor Authentication

The tremendous advantage biometrics provides is incorporating the simplest and most secure user validation: fingerprints. The result is dramatically lower IT burden and increases in user productivity.

Productivity improvements in care delivery at hospitals result from faster access to medical records or prescription authorizations. Aircraft repair centers experience time savings in approving part replacements when every minute counts. Clinical trials increase the validity of patient data gathering by providing irrefutable evidence that doesn't get lost or altered in the field. Anywhere multi-factor authentication is required, fingerprints improve the audit, user and business experience.

## Required Tomorrow: Transaction Proof of Presence

The need to extend security by confirming identity in recurring transactions such as trades or authorizations, is quickly becoming a requirement for many businesses. The only way to achieve continuous compliance down to the transaction level is a fast, easy-to-use mechanism for associating individuals with transactions. The PCI mandate is driving compliance to the transaction level for organizations handling credit card purchases.

### Security and Transaction Proof of Presence

Integrating security at the transaction level requires the least disruptive mechanism possible for end users given the potential impact on user productivity. The choices from a security standpoint are clear: biometric authentication is the only practical method for providing transaction-level strong security without impacting user productivity. Tokens and smart cards are either too bulky or too easily lost or misplaced.

### Compliance and Transaction Proof-of-Presence

The PCI mandate and government regulations driving accountability to the transaction level are primarily due to the need to assign liability associated with security events. If an event occurs, the PCI mandate assumes the card processor or retail store is liable for damages as of the time of the incident, not as of the time of the last audit – which can make a significant difference in penalties and increased card processing fees.

The federal government is also moving toward continuous, transaction-level compliance. Outsourced services require it where those services involve high volume transaction processing. SOX auditors already expect continuous compliance for financial controls: that is, the near real-time availability of financial information for review. It is just a matter of time before this capability makes its way into standard requirements for IT security controls.

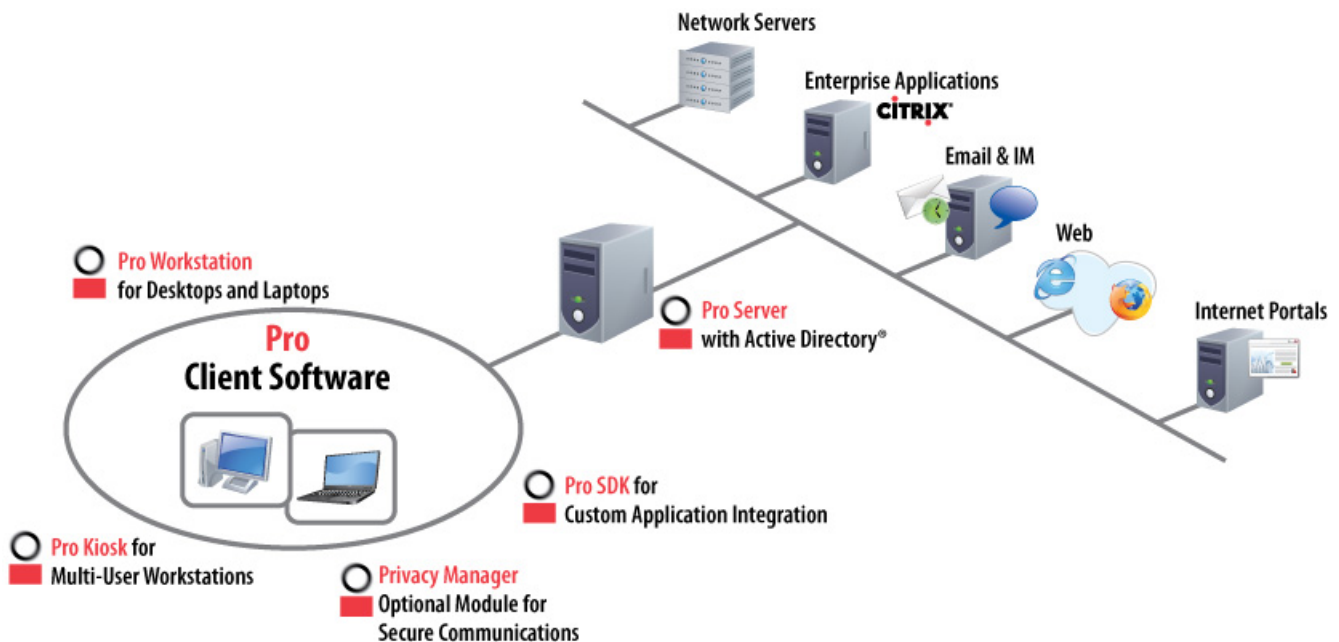
## Business Efficiencies and Transaction Proof of Presence

The value transaction level security provides an organization is that it allows it to automate processes previously thought to be too vulnerable to attack. Enabling cost effective security for transaction-intensive, critical business processes saves the organization time and money.

## How DigitalPersona's Identity Security Technology Works

DigitalPersona's identity security solutions combine a highly accurate fingerprint recognition engine with centralized manageability and a broad set of identity solutions. These solutions work with fingerprint readers built into notebooks or plugged in as peripherals. DigitalPersona's technology is well proven and has been used by more than 90 million people worldwide.

Users set up or "enroll" their fingerprints by simply scanning one or more fingers. DigitalPersona® Pro software on the PC extracts a mathematical representation of the fingerprint called a "template" and uses that for all operations – it does not store any fingerprint images. Templates are then sent to the DigitalPersona Pro server where they are stored in Active Directory so that the user can use fingerprints from anywhere on the network without having to re-enroll at each computer.



When users wish to authenticate (for login, secure communications, multi-factor authentication or transaction proof of presence), they touch the fingerprint reader. A template representing their fingerprint is created and compared against the template that was registered during enrollment. If the templates match, the DigitalPersona Pro client software takes appropriate action, such as writing an audit trail, logging the user in or asking for other authentication information such as a PIN (depending upon policies set by the administrator). Client-side caching of templates ensures that fingerprints can be used even when the computer is not connected to the corporate network.

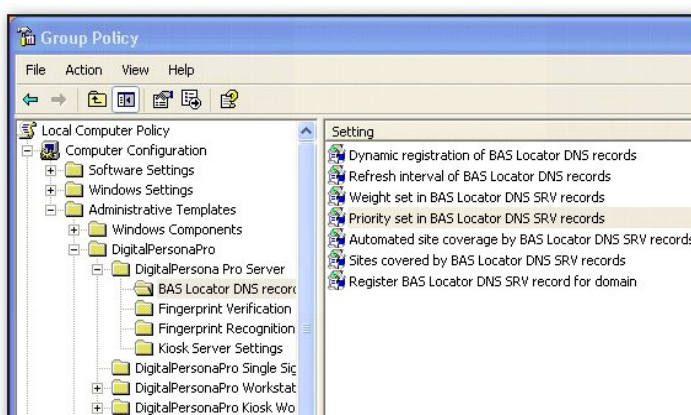
**Simple Deployment on Existing Infrastructure** – DigitalPersona Pro is designed to work with existing PCs, servers, networks, and applications without the need for extensive consulting or custom programming. Client software can be easily deployed wherever needed through existing mechanisms for distributing standard MSI files, including Active Directory Group Policy Objects (GPOs), SMS, or other software distribution tools.

Pro's One Touch® SignOn feature simplifies and secures access to password-protected, third-party software programs and Web sites. Users touch the fingerprint reader to automatically and securely fill in all logon fields, such as user name and password, on any Web site or Windows logon screen. One Touch SignOn administration and application policy settings are used to create and deploy One Touch SignOn templates,

which specify information for logon screens. These user-side templates and policy settings can be set by IT administrators and deployed to large groups of users in one step. One Touch SignOn support includes Java and terminal-based applications. No plug-ins or application server-specific development is necessary. Support includes:

- Microsoft Windows applications
- Web applications
- Mainframe systems and applications
- VPNs, Citrix clients, including support for DOS 32-bit, NFuse, and Java
- Ability to automatically change and modify passwords on dynamic or complex Web pages.

**Integration with Active Directory** – DigitalPersona Pro is certified by Microsoft to extend the Active Directory schema to store biometric data in each user's data records. DigitalPersona Pro uses the native user interface of Active Directory, eliminating the need to learn new tools. Administrators can use the Active Directory Group Policy Editor to create GPOs for tailoring the behavior and functionality of DigitalPersona Pro. This familiar point-and-click interface makes it easy to configure or make changes for groups of users anywhere in the organization's network.



DigitalPersona Pro can be added to new users' computers without disrupting existing users. Similarly, fingerprint logons for new applications can be added at any time.

## Summary

Using a centrally-managed fingerprint identity solution allows IT to satisfy auditors, users, and the business. Fingerprints, which are never forgotten or lost, link users to specific actions that allow the business to know precisely who is accessing what, where and when. This unique combination of accountability and simplicity enhances information security and IT compliance while paying for itself with increased business efficiencies and user productivity.

DigitalPersona Pro takes a platform approach to enable solutions needed today and tomorrow including strong passwords, secure communications, multi-factor authentication and transaction proof-of-presence.

Unlike other approaches, centrally managed fingerprint security solutions result in value return on investment in the following ways:

**Compliance with Certainty** – satisfies identity compliance requirements continuously as auditors move toward increased transparency and audit granularity.

**Security with Simplicity** – helps users do their jobs more easily while increasing protection against system misuse, fraud, social engineering, malware, and hackers.

**Efficiency with Manageability** – pays for security investment by decreasing help desk calls, IT burden, and compliance costs while increasing worker productivity, process automation, and IT utilization of fingerprint-enabled notebooks.

Considering that fingerprint authentication is more convenient, easier to use, more secure and less expensive, the decision to go with fingerprint security technology is an easy one.

\*\*\*\*\*

**Note:** The full names of the regulations and mandates mentioned in this paper include The Payment Card Industry (PCI) mandate, the Health Insurance Portability and Accountability Act (HIPAA), the Gramm Leach Bliley Act (GLBA), the North American Electrical Reliability Corporation Critical Infrastructure Protection (NERC-CIP) mandate, Sarbanes-Oxley (SOX), and the Food and Drug Administration Title 21 Code of Federal Regulations, Part 11 (FDA21CFR11).

## **About DigitalPersona**

DigitalPersona, Inc. is the leading provider of fingerprint identity solutions for enterprises, custom application developers and consumers. Since 1997, the company has offered software and hardware that puts security and convenience at people's fingertips. For end users, DigitalPersona takes the pain out of remembering and typing passwords; the company's business solutions help organizations address growing security, compliance and loss prevention demands.

DigitalPersona's award-winning technology has been used worldwide by over 90 million people, and its biometric software solutions uniquely support the industry's widest array of notebooks in addition to its own line of fingerprint readers. DigitalPersona's solutions are offered by market-leading manufacturers such as HP, Dell, and Microsoft. For more information contact DigitalPersona, Inc. at +1 650.474.4000, or visit [www.digitalpersona.com](http://www.digitalpersona.com).

© 2008 DigitalPersona Inc. All rights reserved. DigitalPersona and One Touch are trademarks of DigitalPersona, Inc., registered in the United States and other countries. All other trademarks referenced herein are the property of their respective owners.