*DigitalPersona Whitepaper*

# Deploying Strong Authentication with Fast and Efficient ROI

September 2010

digitalPersona®

## Strong user authentication is becoming a new standard for security and compliance

In today's IT environment, passwords are no longer a sufficient method for controlling access to sensitive data.

Compliance regulations across many industries are requiring IT professionals to take ever-increasing steps to protect and secure confidential data. In healthcare, the Health Insurance Portability and Accountability Act (HIPAA) mandates strong controls for patient data. In law enforcement, the FBI Criminal Justice Information Services (CJIS) guidelines emphasize the need for strong passwords and alternative authentication methods whenever a user – for example, a law enforcement officer – accesses criminal information data. In other industries and countries, similar regulations are increasing day after day the need for IT professionals to choose and deploy improved user authentication for security and compliance.

## Passwords: an ineffective, expensive solution

The first step many organizations take when asked to enforce improved user authentication is to strengthen their password policies. Users are required to use longer and more complex passwords, change them more frequently, use different passwords for each business application and so on.

Unfortunately, instead of strengthening security, such rules often have the opposite effect. Market data shows that users inevitably:

- Write down their passwords on Post-it® notes.
- Use the same password for many applications.
- Share passwords with colleagues.

In addition, passwords cause significant costs to the organization that often go unnoticed. Every time there is a password, users will find a way to forget it. This translates into costs in terms of Help Desk calls, support and lost user productivity[1].

The bottom line: stronger passwords will not help your organization improve security yet they will trigger significantly higher costs.

## Choosing strong authentication: now what?

An increasing number of organizations have deployed, or are considering, improved authentication options that include the use of alternative methods to verify a user's identity when they log on to the computer or to enterprise applications[2].

According to Aberdeen, best-in-class proactive organizations can often be distinguished from less advanced, reactive companies by the value they place on protecting the organization and their assets. Such businesses are increasingly deploying strong authentication as a means to improve security and meet industry best practices, and not simply to comply with external regulations[3].

Choosing the most appropriate authentication solution, however, isn't always straightforward. There are many options available and comparing products can be tricky. So, how should you decide which authentication solution is right for your organization?

[1] *Toolkit: Evaluating Enterprise Options for Managing Passwords*, Gartner, November 2006.

[2] *Strong User Authentication: Best-in-Class at Assuring Identities*, Aberdeen Group, March 2008.

[3] Id. at 2.

Some of the key elements to consider in your analysis and evaluation are:

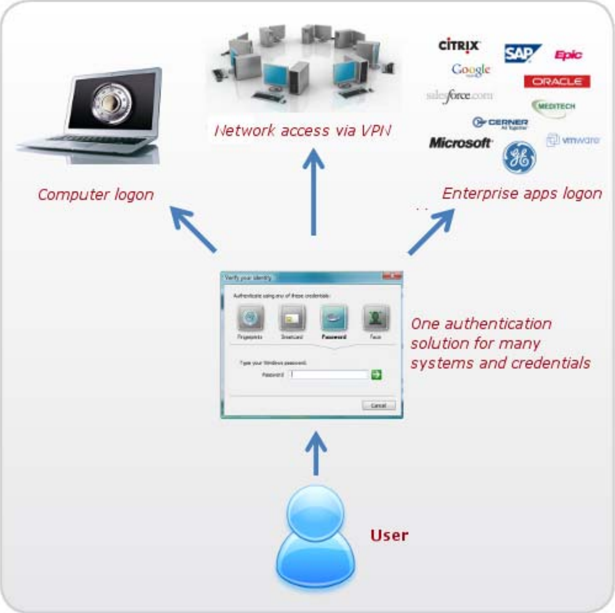
- Is this a single, 'silo'd' security application or is it part of a suite of solutions that can be expanded over time as your needs grow?
- How quickly will this solution generate a tangible Return on Investment (ROI)? Can it pay for itself by freeing my IT staff to focus on other issues?
- Will this solution help me keep costs down with a low Total Cost of Ownership (TCO)?

## Creating a new authentication paradigm across platforms and applications

Substituting passwords with alternative authentication methods establishes a different, and ideally simpler, way for users to verify their identity within the enterprise.

The power of any authentication method – and one of the reasons why passwords have become so popular – comes from the number of applications and purposes it supports. Users' identities do not change when they unlock their encrypted laptop, remotely connect to the network via VPN, or they log onto enterprise applications. IT managers should expect alternative authentication methods to support such flexibility and offer broad interoperability.

This is why best practices in implementing strong user authentication recommend adopting solutions that provide broad support across platforms, applications and credentials[4].



When comparing best-in-class organizations against other companies, Aberdeen Group found that best-in-class companies are 31% more likely to implement a single back-end solution that manages various credentials (e.g. fingerprints, smart cards, tokens) through their lifecycle. At the opposite side of the spectrum, deploying separate authentication methods for different purposes (e.g. OTP tokens for two-factor VPN access, PKI for digital signature, etc.) can be confusing and increase IT burdens[5].

## Strong authentication brings high ROI

Many company success stories[6] have found that strong authentication solutions can deliver a high Return on Investment in at least two ways:

- By reducing the risk of security breaches
- By reducing password-related costs

In a recent study, Aberdeen Group estimates that security breaches can cost as much as $640,000 per

[4] Id at 2.

[5] Id. at 2.

[6] Id at 1 and 2.

incident[7]. Those costs are primarily due to legal expenses, lost revenues, bad PR and loss of customer satisfaction.

That same study found that implementing strong authentication solutions can help reduce the exposure to security breaches. More than half of best-in-class organizations decreased the number of security related incidents and 80% reduced the amount of human error related to security[8]. Preventing just a handful of security incidents can easily add up to millions of dollars of savings per year.

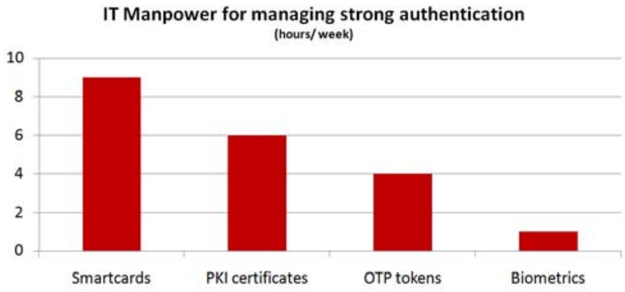
Gartner estimates that password-related Help Desk calls – such as password resets – cost an average of $17 per call and that 30% of the overall Help Desk call volume is typically associated with passwords[9]. Many companies report password reset costs that are even higher.

Examples from organizations that have deployed solutions such as password management and Single Sign-On (SSO) show that these solutions can help reduce support costs by 70%-90%[10]. For an organization with 1,000 users, this would represent cost savings of as much as $54,000 per year.

## Achieving low Total Cost of Ownership (TCO)

The selection of the optimal authentication solution can dramatically impact the solution's Total Cost of Ownership (TCO). Aberdeen reports that more than a third of best-in-class organizations in strong authentication have managed to decrease the total management costs related to user authentication, while 31% of "laggard" companies have experienced an increase in those costs over the last twelve months[11].

The choice of authentication credentials can dramatically impact the administrative burden associated with managing alternative methods. Studies from Datamonitor and Microsoft reveal that choosing the "right" credentials can lower the IT resources required for ongoing management by as much as 90%[12].



## The solution: DigitalPersona® Pro

DigitalPersona Pro provides small businesses and enterprises with a powerful, flexible authentication solution that combines multi-credential authentication with a centrally-managed suite of security applications, including Full Disk Encryption, Two-Factor VPN Authentication, Single Sign-On, Digital Signature and more.

Key benefits of DigitalPersona Pro include:

- One solution for many credentials, including fingerprint, face recognition, smart cards,

[7] *Full Disk Encryption On the Rise*, Aberdeen Group, September 2009.

[8] Id. at 2.

[9] Id. at 1.

[10] Id. at 1. See also *Applications at Their Fingertips*, Federal Computer Week, August 2004.

[11] Id. at 2.

[12] *The ROI for Enterprise Smart Cards*, Datamonitor and Microsoft

one-time (OTP) tokens and smartphones. DigitalPersona Pro takes advantage of fingerprint readers that are built into notebooks or attached as peripherals and supports a wide range of smart cards and OTP devices.

- Native integration of strong authentication into a suite of powerful applications for data protection, including Full Disk Encryption, BIOS-level security[13] and encryption for email and documents.
- Two-Factor VPN authentication for secure remote access. DigitalPersona Pro supports all RADIUS-based Virtual Private Networks such as Cisco, Juniper, Check Point and others.
- Single Sign-On to all enterprise applications, including Citrix, Web apps, Windows applications, legacy green-screen terminals and more.
- Powerful emergency access recovery to securely "rescue" users who are locked out of their PCs, even when a network connection is not available.
- Ability to roam users' credentials across computers, providing consistent strong authentication without per-machine setup.
- Support for shared workstations, such as financial institutions, police vehicles or kiosks in hospitals.
- Flexible deployment options that include a self-contained configuration, as well as Active Directory-based management.
- High security with FIPS 140-2 compliant encryption for user data and credentials.
- High Return on Investment and low Total Cost of Ownership with savings over 50% in out-of-pocket costs over individual solutions.

DigitalPersona's award-winning technology has been used worldwide by thousands of companies and over 100 million users for security and compliance. Customers range from small businesses to the US Department of Defense, from hospitals to banks.

DigitalPersona powers HP ProtectTools, the security suite preloaded by Hewlett-Packard on millions of business notebooks and desktops every year. Now you can use DigitalPersona Pro to centrally manage HP ProtectTools-enabled computers or any mixed environment of HP ProtectTools and DigitalPersona Pro client software.

## Questions? Contact us!

For more information about DigitalPersona Pro, visit www.digitalpersona.com or contact us at:

- Email: sales@digitalpersona.com
- North America contact: +1-650-474-4000
- EMEA contact: +44-203-286-4004

Free trials are available.

## About DigitalPersona

DigitalPersona, Inc. is a global provider of authentication and endpoint protection solutions that make security simple, practical and affordable for businesses of all sizes. The company helps enterprises, government agencies, custom application developers and independent software vendors to efficiently address growing security, compliance and fraud-prevention demands. DigitalPersona's award-winning technology is offered by market-leading computer

[13] Available on select computers.

manufacturers and solution providers around the world.

**Disclaimer**

**THE INFORMATION IN THIS DOCUMENT IS PROVIDED FOR INFORMATIONAL PURPOSES ONLY. ALL STATEMENTS, INFORMATION AND RECOMMENDATIONS IN THIS DOCUMENT ARE BELIEVED TO BE ACURATE BUT DIGITALPERSONA MAKES NO CLAIMS, PROMISES OR GUARANTEES ABOUT THE ACCURACY, COMPLETENESS OR ADEQUACY OF THE INFORMATION. DIGITALPERSONA SPECIFICALLY DISCLAIMS ALL WARRANTIES OF ANY KIND, EXPRESS OR IMPLIED. USERS MUST TAKE FULL RESPONSIBILITY FOR THEIR APPLICATION OF ANY PRODUCTS.**