

Simplified Identity Management, Stronger Authentication

Leveraging existing infrastructure to streamline identity
management across the enterprise

A DigitalPersona Whitepaper

May 2003



digitalPersona

Simplified Identity Management, Stronger Authentication.....	1
Introduction	2
Identity Management	2
Traditional Definition- Management of User Accounts (moves, adds, changes)	2
New Focus- Management of Identity Data (passwords, biometric data, tokens...)	3
The Identity Management Problem	3
Credentials Managed by End-Users	3
Traditional Identity Management Solutions	4
Account Management Solutions.....	4
Password Management Solutions	4
Strong Authentication Solutions	5
Integrated and Improved Identity Management.....	5
Fingerprint Sign-On	5
Active Directory enabled Fingerprint SignOn	6
Summary	7

Introduction

Organizations have made tremendous investments over the past decade in securing against outside attack by hackers and viruses. This adoption was fueled by obvious, well-publicized threats, and cost effective technology (i.e. firewalls) to reduce risk. While the security threat posed by insecure identity management is apparent, there has not been a cost effective solution that tackles the usability and security issues - until now.

The growing need for better control over access to sensitive data has shifted the definition of identity management solutions for many enterprises. The traditional definition focused on account management where today's requirements have broadened the need to include credential management and stronger authentication. These needs are sometimes referred to as the 3 A's (Authorization, Authentication, and Administration).

Research firm IDC defines Identity management as "like cycle management of user identity data, including password synchronization across multiple applications, single sign-on, and policy-based access control."

Account management, password management, and stronger authentication solutions attempt to address fundamental identity management issues from different vantage points.

- Account management solutions consolidate the management of user accounts and privileges (authorization and administration)
- Single Single-on solutions consolidate and help manage the number of passwords for each user.
- Stronger authentication solutions typically increase the security of a limited number of accounts' identities through additional credentials (e.g. tokens), without consolidating the number of accounts.

These disparate enterprise systems are complex, partial solutions to identity management and are typically difficult and expensive to integrate and maintain.

The remainder of this paper describes:

- The shifting definition of identity management
- Why identity management has become increasingly important,

- Traditional identity management solutions and their weaknesses, and
- How you can reduce operational costs, achieve improved identity management and security, using well-integrated products - today.

Identity Management is the life cycle management of user identity data including:	
Password Synchronization	Single Sign-on
Secure Authentication	Policy-based Access Control

Figure 1. Identity Management Definition - IDC

Identity Management

Traditional Definition- Management of User Accounts (moves, adds, changes)

Traditional identity management solutions consolidate the management of user accounts and privileges (authorization and administration) across multiple applications.

According to Forrester Group, the average Fortune 2000 Company has over 180 directories. The benefits from globally managing a user are significant. As employees join, move within and leave the organization, the various user accounts they access must be created, changed, and removed.

Identity management tools allow administrators to consolidate the administration of the users' various accounts into one tool, providing more reliable and cost-effective service. While traditional identity management solutions improve the manageability of identities they do not secure them.

New Focus- Management of Identity Data (passwords, biometric data, tokens...)

The growing need for better control over access to sensitive data has shifted the goal and definition of identity management for many enterprises. As expressed by IDC, identity management is much broader than the original definition and should be viewed as “life cycle management of user identity data, including password synchronization across multiple applications, single sign-on, and policy-based access control.” It includes various types of identity information – including passwords, user IDs, biometrics, and tokens. These data are referred to as credentials and are the basic elements of user authentication; the process of proving identity.

This leads to the critical link between identity management and secure authentication; improperly managed credentials lead to compromised user authentication (identity theft) and unauthorized access. Protecting access to sensitive data is mission critical to many organizations and the overall goal of information security.

With this in mind, the next sections present i) the need for identity management, ii) weaknesses that have limited the deployment of traditional identity management solutions, and iii) how fingerprint based solutions tackle both the end-user convenience and administrative control requirements of identity management.

The Identity Management Problem

Credentials Managed by End-Users

Accounts and access rights to these accounts are secured and maintained through administrative control by trusted IT professionals. Although security administrators control authentication policies, such as password size, expiration, etc., credential management (i.e. creation and secrecy of each password) lies entirely in the hands of each end-user. This presents two critical and intertwined problems related to information security and user productivity and support costs.

Information Security (a.k.a. The Problem with Passwords)

Administration, Authorization and Authentication (or sometimes referred to as the “3A’s”) are essential to securing access to corporate information. The lack of control by trusted security administrators over user credentials, presents a pervasive and

extremely weak link in the security chain. In this model, network security relies on the diligence of every end-user to properly manage their passwords, tokens, smartcard, etc. While most employees can be trusted to follow policies, it takes only one mismanaged password from any user to compromise the entire network or a key database.

“The biggest threat to the security of a company is not a computer virus, an unpatched hole in a key program or a badly installed firewall... The weakest link in the chain is the people” - Kevin Mitnick; Oct 2002, BBC Interview

Passwords are often found written on Post-it® notes at users’ desks, given out to others, and in many cases are easy to guess. Many people use the same password everywhere, and use simple variants against a common root if asked to change.

The only approach to solve the problem – requiring frequent changes and complexity requirements – tends to backfire since people can’t remember the new passwords and are even more apt to write them down. Password security policies rely on end-user cooperation, and strict policies motivate users to compromise security. Those who comply will generate higher support costs due to forgotten passwords. It’s a catch-22, with stricter policies actually lowering overall security.

Security auditing and break-in forensics are also crippled because one can always say that someone else pilfered their password and there is no way to prove otherwise. Getting the password to merely one person within an organization, even the receptionist, allows a hacker to get a foothold within the firewall.

The following examples indicate how large a problem this is:

- <http://zdnet.com.com/2100-1105-976888.html> - “The 2002 NTA Monitor Password Survey found that the typical intensive IT user now has 21 passwords, and has two strategies to cope, neither of which is advisable from a security standpoint: they either use common words as passwords or keep written records of them. The survey found that some of these heavy users maintain up to 70 passwords. Forty-nine percent write their passwords down, or store them in a file on their PC. The research shows

that 84 percent of computer users consider memorability as the most important attribute of a password, with 81 percent selecting a common word as a result.”

- <http://news.com.com/2009-1001-916719.html> - “[A recent study] found that four out of five workers would disclose their passwords to someone in the company, if asked. That's the good news. Another study by the same company found that nearly two-thirds of the workers polled at Victoria Station in London gave the pollster their passwords when asked. Their reward? A cheap pen.”

User Productivity and Support Costs

Arguably, most users will securely manage their identity data (credentials); creating secure passwords and hiding their passwords and/or tokens from others. Unfortunately these conscientious users will inevitably forget their password or token and generate a support call. As users are given access to more accounts, the number of passwords they must manage correspondingly rises.

Forgotten passwords can make up to 30% of help desk calls costing between \$50 - \$150 each.

In many cases, the cost is much more than the cost of the support call.

- Call centers, or any customer facing operation where employees repeatedly login and logout of various applications while customers wait.
- Mission critical operations such as in hospitals where medical records must be quickly accessed from a shared PC at a nurses station.

Traditional Identity Management Solutions

Account Management Solutions

Account management solutions, sometimes called Meta directories, create a common management tool for user accounts and privileges (authorization and administration) across all, or some portion, of the applications within the organization.

These products are designed to increase productivity at the administrator level for environments that have an excessive number of moves, adds and changes generated by a i) large amount of applications and ii) a dynamic user base.

Account management products may use custom software agents for each application directory to collate information, or they may require that applications are developed using their directory and management infrastructure. Either method requires custom integration and often cannot support all of the key applications in an organization.

Account management products typically introduce a separate global directory and management tools and do not integrate into the existing network directory. These solutions do not address password management, and those that do require massive custom development.

Password Management Solutions

Password management solutions attempt to increase end-user productivity and lower support costs by simplifying the job of managing numerous, complicated password credentials. Most password management solutions are based on stand-alone databases and management tools that do not easily interface with the network directory and its management tools. The following is an overview of several different types of password management solutions.

Single Sign-On

Single Sign-On (SSO) products simplify the management of password credentials by allowing a single password to provide access to all applications.

Ideally, this would eliminate the management of all password credentials, except for one, and give the user free access to all applications with only one logon.

In reality, there are several drawbacks that limit the viability of SSO for many companies. Most SSO solutions require an administrator / programmer to perform complex scripting for each application to be supported. This work is often multiplied over time as applications are updated and their logon screens change. Furthermore, many security experts consider SSO less secure than using separate passwords. This is because SSO still relies on the end users to create and maintain a secure password and only one password is required to access all of the users' accounts (sometimes called “Single Break-In”). In the end, the combination of high cost of ownership and continued reliance on an end-user to securely manage a password limit the viability to all but a few organizations.

Password Self-Reset

Password self-reset solutions have recently gained a lot of attention in light of the growing password problem. These solutions reduce help desk calls for forgotten passwords by allowing users to reset their own passwords without calling for support.

Password self-reset products do not address the source of the security problem; end-users still must create and maintain (manage) a number of secure passwords.

Additional downsides of these solutions are:

- (1) they are not turn key and often require immense professional services projects to support the integration effort required for each application, and
- (2) while they do significantly reduce help desk costs associated with forgotten passwords, end-user productivity is still impacted as they must perform the password reset.

Strong Authentication Solutions

The market for stronger authentication solutions has been primarily driven by the need to secure access from outside the firewall. While the need to secure access has expanded far beyond remote users, these solutions have not addressed the operational requirements for a broadly deployed authentication solution.

These solutions typically use a token/smartcard (something you have) in addition to a password (something you know) to authenticate users. This is known as “two factor” authentication. Increasing the number of required credentials (factors) is a broadly accepted method of increasing security.

Token/password based authentication solutions have been commonly used but limited to where the added security can justify the cost and burden. There is a large upfront and ongoing cost to deploying and managing tokens. Users often forget them or leave them at their desk. Traditional strong authentication solutions also do not support all applications and do not tightly integrate into the native network directory and management infrastructure. These issues have limited the deployment of token-based authentication products only to users who require secure remote access.

Integrated and Improved Identity Management – U.are.U Pro for Active Directory

Account management, password management, and stronger authentication solutions attempt to address fundamental identity management issues from different vantage points. These disparate enterprise systems are complex, partial solutions to identity management and are typically difficult to integrate and maintain. The emergence of fingerprint authentication solutions for information systems and their integration into the latest network directory infrastructure has enabled an opportunity to reduce operational costs, achieve improved identity management and security, using well integrated products - today.

Fingerprint Sign-On

Simply put, the security benefit of fingerprint authentication systems, such as U.are.U Pro, are to eliminate the reliance on users to manage their authentication credentials (passwords, tokens, etc).

A fingerprint match can be a proxy for password entry into all logons (Windows, webpage, Windows applications and legacy systems) via an extension to AD, and requires no programming or back-end system integration. The administrator or user can train any logon screen to map the username/ password fields to be filled in automatically after a valid fingerprint match.

Furthermore, in its next release, U.are.U Pro will enable an administrator to train any “password change” dialog to fully randomize passwords upon a password change request by the application. When this feature is enabled, it means that users will no longer need to know their passwords, further removing the possibility of a social engineering attack, and that passwords can be arbitrarily complex and long which will foil password-cracking programs.



Fingerprint authentication raises the bar of security over the use of passwords while in the corporate network. Providing a convenient replacement for passwords is the primary objective of U.are.U. However U.are.U also accomplishes strong authentication. Each class of authentication methods (something you know, something you are, and something you carry) solves different parts of the security puzzle. For special scenarios in which greater threats are identified, such as remote access and high profile users, U.are.U allows the administrator to layer authentication so that both a fingerprint and the Windows password is required. Obviously this provides provably stronger authentication than a password alone.

Active Directory enabled Fingerprint SignOn – High Value: Low TCO

Fingerprint based identity management solutions tackle both the end-user convenience and administrative control requirements of identity management. Combining U.are.U Pro fingerprint authentication with Active Directory creates a

powerful ID management and security solution with much lower TCO than stand-alone, disparate ID management and authentication solutions. Active Directory provides a large-scale identity management infrastructure that provides a framework for enterprise applications, allowing consolidation of disparate identities and databases using the already existing password-based infrastructure. U.are.U Pro provides secure and convenient authentication for users who access their Active Directory accounts. U.are.U takes passwords, and their associated abuses, out of the hands of end-users.

Furthermore, U.are.U Pro extends the identities managed by Active Directory to all enterprise applications and websites - even if they are not yet designed to leverage the Active Directory management infrastructure. This is done through a secure mapping of each of the users' identities to their fingerprint credentials, managed within their AD Account.

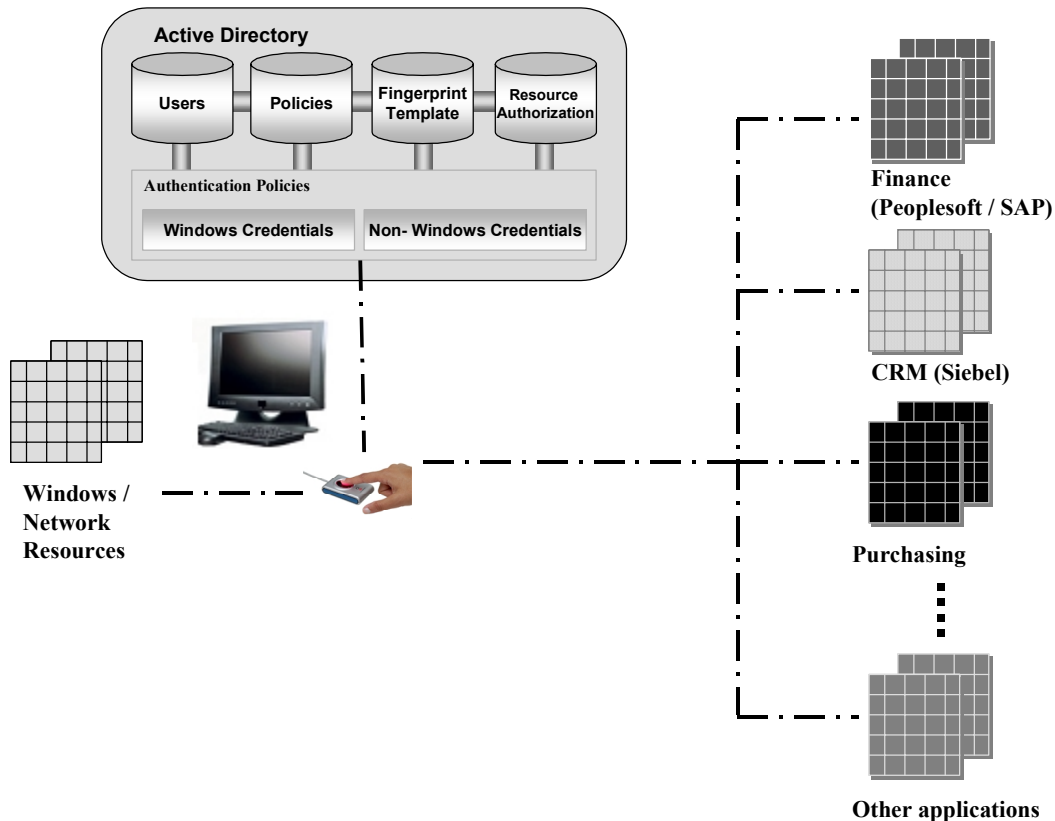


Figure 2 DigitalPersona consolidates identities across the enterprise

Key benefits of a combined DigitalPersona U.are.U Pro and Active Directory solution include:

- Increased Security with Quick ROI.
- Consolidate management of authentication for all identities.
- Fast, secure access to all Active Directory and Application accounts.
- Eliminate reliance on end-users to manage and remember secure passwords.

- Seamless integration.

The benefits of the fingerprint authentication coupled with ID management are significant. Furthermore, U.are.U Pro for AD is much less complicated and has dramatically lower TCO than stand-alone, disparate ID management and authentication solutions.

Figure 3: Capability Matrix

	Traditional Identity Management	Active Directory	DigitalPersona (fingerprint authentication)	Active Directory with fingerprint authentication
Account Management	<ul style="list-style-type: none"> ▪ Complex ▪ Expensive 	<ul style="list-style-type: none"> ▪ Simplified 	--	<ul style="list-style-type: none"> ▪ Simplified
User Passwords /authentication	<ul style="list-style-type: none"> ▪ Limited Control ▪ High risk 	--	<ul style="list-style-type: none"> ▪ Increased security ▪ Greater administrative control ▪ More convenient 	<ul style="list-style-type: none"> ▪ Increased security ▪ Greater administrative control ▪ More convenient

U.are.U Pro for AD utilizes the Active Directory database for storage and management of user data. This dramatically reduces deployment, administration, and maintenance costs over solutions that require a separate user database that must be installed, replicated, backed-up, and maintained across the enterprise. Authentication solutions that require disparate “shadow databases” often become more of an administrative drain than an identity management solution. With U.are.U Pro for AD, the native Windows user record is extended and the encrypted U.are.U user data is automatically replicated throughout the enterprise along with the existing user data. New Windows user accounts are automatically added to U.are.U Pro, existing accounts are managed through the AD management tools, and deleted accounts are automatically removed from U.are.U Pro for AD.

In addition, U.are.U Pro for AD server software takes advantage of many of the Windows 2000/2003 services. For example, DNS lookup, site

configuration, server load balancing, etc. are performed through the standard services provided by Windows 2000/2003 servers.

Summary

Identity Management has become a challenging issue for many organizations. Many different approaches are available for addressing identity management needs, but they require trade-off between complexity and security. With U.are.U Pro for Active Directory, fingerprint authentication replaces passwords for end-users with the user ID and password credential managed securely, “behind the scenes,” through Active Directory. The benefits of the approach are end-user convenience, tighter security and the lowest TCO in the identity management space.