A More Secure Front Door

ESSO and Strong Authentication

January, 2006

ESSO and Strong Authentication

Introduction

In recent years, enterprise single sign-on (ESSO) has emerged as an easy, smart and affordable way for organizations of all types and sizes to strengthen IT security while supporting user productivity. With the advent of more stringent government regulations, organizations are seeking ways to further strengthen IT security by incorporating stronger passwords and in many cases an additional form of authentication, such as a security card or token or even finger biometrics.

The idea behind using an additional factor beyond a password provides strong authentication so that each computer on an organization's network has a stronger "front door" against entry by unauthorized users. However, the use of these increased security measures has an impact across the organization, both on all computer users as well as the Help Desk staff who need to support these users. ESSO alleviates the inconvenience not only of a multiplicity of stronger passwords to access applications, but also integrates with strong authentication to ensure that every "front door" in the organization is as secure as possible.

But which authentication option is right for you and your organization? And how easily can it be integrated with your ESSO solution? These are just two of the many questions to consider as you evaluate strong authentication choices. This white paper explores these questions and addresses how organizations can achieve strong authentication with ESSO — easily and affordably — to increase their security levels dramatically without creating inconvenience for either IT staff or end users.

The Rise of Strong Authentication

Not long ago, authentication technologies such as biometric fingerprint scanners and smart cards were only found in top-secret government facilities and James Bond movies. Not anymore. According to IDC, identity and access management was a $2.21 billion market in 2003, and it is expected to grow to $3.5 billion by 2008. In a poll conducted recently by *Network Computing*, 62% of respondents stated that they were planning to implement more rigorous security measures beyond simple passwords.

There are several reasons for this growing interest in strong authentication, including:

Increased access

Corporate computing environments are no longer closed, self-contained entities. As more internal and external users access corporate applications — local, host-based, and Web-based — in more ways from more kinds of devices, the opportunities for unauthorized access have grown dramatically.

Increased awareness

Crippling viruses, worms, and spyware and even internal attacks have alerted corporate executives to the very real threats to their information assets — and the potentially grave consequences to their business operations, customer relations, and financial performance.

Increased regulation

Within the last several years, governments around the world have mandated a series of new IT security measures and processes as part of such acts as Gramm-Leach-Bliley, Sarbanes-Oxley, and Health Insurance Portability and Accountability (HIPAA) in the U.S, and the Data Protection Act in the UK. Industry regulations, such as Basel II, FDIC, and the U.S. Code of Federal Regulations (CFR), as well as industry standards, such as BS7799 in the UK and BS7799-2 and ISO 17799 worldwide, are also mandating stronger authentication. Organizations and corporate officers must comply with these regulations or be subject to fines, legal action, and/or negative customer reaction.

Analysts are also leading the move to strong authentication. A recent report by Gartner ("Assess Authentication Methods for Strong System Security," August 2004) outlines two primary recommendations for increasing security and reducing password issues: 1) implement password management; and 2) utilize strong, two-factor authentication.

The value of strong and two-factor authentication with ESSO

On the face of it, the logic for implementing strong, or two-factor, authentication with ESSO is self-evident: it provides greater protection from unauthorized access. Like the secure vault inside a locked bank, the second authentication factor provides extra protection where it is most needed.

But there are other, equally compelling reasons to implement strong, or two-factor, authentication with ESSO. They include:

The elimination of passwords.

ESSO greatly reduces the problems and costs associated with password management. By adding a stronger authentication factor, organizations can eliminate the need for users to deal with passwords entirely. At the same time, it puts greater password control in the hands of the IT organization. As an Imprivata OneSign healthcare customer remarked recently:

> *"We are planning on rolling out fingerprint biometrics to all our users —- ER physicians, nurses, radiologists — as soon as possible. That way, they will only have to remember their user name, but not a password. This will save our healthcare professionals a lot of time. It will also allow us to create and control passwords on the back end, giving us even greater security."*
>
> – Stefan Hopper, Chief Information Officer, Gateway Health System

A better, faster ROI than one alone.

Some authentication technologies can be costly to deploy, and thus a difficult expense for some organizations to justify. By combining affordable ESSO and a stronger or second authentication factor, organizations can earn a better, faster ROI as they reap the added benefits and cost-savings of password management, such as lower help desk costs and enhanced user productivity.

Proven regulatory compliance.

Some organizations have implemented measures, such as strong password policies, designed to comply with regulations such as HIPAA and Sarbanes-Oxley, but lack objective, documented proof that those measures are being followed and enforced. This means they still may be at risk of being found non-compliant. Strong authentication with ESSO provides demonstrable compliance in the form of audit logs that record all relevant activity.

Leading authentication methods

As the demand for stronger authentication measures has grown, so have the solutions available to organizations. The following are the most popular authentication methods in use today:

Passwords

The original and simplest authentication method, passwords became popular because they were simple and relatively effective. As long as users kept their passwords secret, no one else could gain unauthorized access to applications. However, the proliferation of applications requiring passwords made it either harder for users to remember multiple passwords, or the user-created passwords were often too simple or reused, making them easy to crack.

Strong Passwords

To remedy the problems of simple passwords, many organizations began mandating the use of strong passwords — passwords that are more complex, utilizing numbers and special characters rather than just letters. Unfortunately, strong passwords were often too complex for users themselves to remember, resulting in an upsurge of costly calls to help desks for assistance. This in turn has a negative impact on user productivity as they are prevented from doing their work while waiting for password

resets. Worse yet, users may leave passwords written down where anyone could steal and use them.

ID Tokens

ID tokens are small devices that generate numeric codes that validate access for a limited time or a single use. Some ID token systems, as an extra measure of protection, require the user to type a challenge string into the token before the passcode is generated. Many combine a PIN to be entered alongside the OTP (one-time password) for two-factor authentication. Leading ID token vendors include RSA, Secure Computing and Vasco.

Smart Cards

As their name implies, smart cards have built-in intelligence. They can contain a variety of data for authentication and security. Smart cards cannot be tampered with, and they can perform multiple functions; a single smart card can serve as an employee ID badge, building access card, Windows credential store, and application password provider. Companies such as ActivCard, Axalto and Gemplus offer smart cards. Similarly, USB tokens from these vendors and others such as Aladdin offer an intelligent and easy-to-use readerless security alternative.

Passive Proximity Cards

Similar to smart cards, passive proximity cards are contactless access control cards that provide authentication data via radio frequency (RF) technology. When a passive proximity card is waved near a card reader, the reader collects user data from the card to authenticate the identity of the cardholder. Like smart cards, passive proximity technology can be embedded into traditional employee ID badges and building access cards. Passive proximity cards are offered by companies such as HID, MIFARE and Indala.

Active Proximity Cards

Active proximity cards include a wireless radio transmitter (worn by the user) that stays in constant communication with a transceiver connected to the user's workstation whenever the user is nearby. When the user steps away from the workstation, the communication is broken and the computer automatically locks, thereby ensuring full-time access control. One of the leading active proximity card vendors is Ensure, maker of the XyLoc card.

Finger Biometrics

Finger biometrics authenticate users with something that is uniquely theirs — their fingerprints. Users enroll one or more fingerprints via a scanner, which then records aspects of the fingerprint associated with each user's identification information. Thereafter, when logging in, the user's finger is scanned and compared to the file to complete the authentication process. Finger biometrics are offered by companies such as UPEK and are increasingly built into products such as the ThinkPad T42.

All of the authentication methods listed above can help prevent unauthorized access to corporate information systems. There are, however, other aspects to consider, including the specific benefits of each method for users, IT departments, and regulatory compliance, as well as purchase and deployment costs. By understanding those benefits and costs and evaluating them in light of your organization's unique needs, you can choose the strong authentication method that will work best for you.

Comparing Strong Authentication Methods

Every organization wants to prevent unauthorized access to its information assets — and all organizations can benefit from the use of strong authentication. But individual requirements vary greatly. For example:

- A **behavioral health office** needs an authentication method that allows for shared workstation use while protecting confidential patient records in compliance with the Health Insurance Portability and Accountability Act (HIPAA). If the office is small or medium-sized, its strong authentication solution must also be affordable to purchase, deploy, and use.

- A large, **publicly-traded financial services corporation** needs a method that can be cost-effectively deployed enterprise-wide. It also needs to ensure compliance with Section 404 of the Sarbanes-Oxley Act, which mandates the use of internal controls to protect the integrity of the financial reporting mechanism and a way to prove the quality of those controls.

- A **technology firm** with substantial intellectual property assets needs to maintain stringent access control of R&D files, but may also need to make remote access both convenient and secure for traveling sales representatives.

- A **law enforcement organization** needs a method that can be easily used by non-desk workers in an open office environment.

Key factors to consider

In addition to considering your organization's unique security requirements, it is important that you weigh the benefits and costs of different strong authentication choices. These include:

IT benefits

Is the authentication method easy to deploy enterprise-wide? Will it require additional IT resources? Is it easy to integrate with existing ESSO solutions? Does it support centralized management?

User benefits

Is the authentication method easy to use? Will end users accept the new process? Will it increase user productivity? Does it put an undue burden on users? Does it require them to carry a device that could get lost or damaged?

Compliance benefits

How fully does the authentication method support the regulatory requirements of Sarbanes-Oxley, Gramm-Leach-Bliley, HIPAA, CFR, Basel II, the UK's Data Protection Act, or BS7799? Does it go beyond simple access control by tracking authentication events to support auditing requirements and objectively prove compliance?

Industry-specific benefits

Are there aspects of the authentication method that make it better suited for certain industries or functional areas?

Purchase cost

Is the cost of the authentication method worth the resulting improvement in security? Is there a cost per user that will grow every time a new user is added?

Deployment cost

Does deployment require physical installation by a technical person on every workstation at every site? Does the IT organization need to write custom code, add middleware, or incur other hardware or software costs to integrate the strong authentication method with ESSO?

The matrix below illustrates how each of the major authentication methods compare to each other on these key factors:

Cost/Benefit Comparison of Leading Authentication Methods

Type	Ease of Management* for IT	Ease of Use for Employees	Compliance/ Security Level	Cost to Purchase	Cost per User to Deploy
Password	Medium	Medium	Low	$	$
Strong Password	Low	Low	Medium	$	$$
ID Token	Medium	Medium[1]	High	$$	$$
Smart Card and USB Token	Low[2]	Medium[1]	High	$$	$$$
Passive Proximity	Medium	Medium[1]	Low[3]	$$$[4]	$
Active Proximity	Medium	High	Low[3]	$$$$	$$
Finger Biometrics	High	High[5]	High	$$$	$

*Time and Resources involved to deploy and maintain the technology or to support the end user

Notes:

1. Device needs to be carried by user and is subject to loss or damage.
2. IT needs to manage devices that are often lost, forgotten, or accidentally damaged.
3. Unless combined with another authentication factor
4. Cards are inexpensive (~$1/each), but required readers are not.
5. Fingerprints can never be lost or forgotten.

By doing a cost-benefit analysis of the different strong authentication approaches, you can determine which technologies best meet your organization's needs and preferences. For example:

- If ease of use for employees and IT staff is a top priority, biometrics or active proximity cards might be your best choice.

- If your organization is large or growing rapidly, you may want to keep per-user deployment costs low by selecting passive proximity cards.

- If your organization is in a sensitive industry that demands strong security above all else, and the user population is small or not expected to grow sharply, then smart cards or ID tokens might make the most sense.

- If your security requirements vary by location or department, you may prefer to implement different authentication methods based on user sophistication and needs.

Integrating Strong Authentication with ESSO

Integration costs and resource requirements

Selecting a method of strong authentication for your company is only one step toward ensuring strong enterprise access security. To gain value from a strong authentication solution you need to integrate that second form of authentication with a strong, smart and affordable ESSO solution.

For some ESSO solutions, implementing strong authentication requires additional software, servers, middleware, support and user interfaces. And some ESSO solutions only support certain forms of authentication.

Implementing strong authentication with OneSign

Imprivata OneSign is different. Imprivata OneSign is an affordable, non-intrusive appliance that provides ESSO for all applications — Web, client/server and legacy applications. Through a unique, centralized approach to password management, OneSign makes secure SSO services quick to deploy, convenient to use, and easy to administer. As a result, customers benefit from increased productivity, higher user compliance and lower help desk costs. OneSign makes it simple and practical for companies of all sizes to adopt and enforce password policies.

OneSign is uniquely designed to work easily with the full spectrum of authentication methods. For example, the following steps describe the **entire process** of **deploying** fingerprint biometrics and enrolling a user with OneSign:

1. Plug a fingerprint scanner into the PC's USB connection.

2. Follow the Windows prompts. There are no drivers to install.

3. Shut down and restart the computer to invoke a OneSign authentication.

4. Follow the OneSign prompts to enroll one or more fingerprints.

5. At the prompt, scan the finger.

6. Click "Done."

For all subsequent user logins:

1. Users place finger on fingerprint scanner attached to PC
2. User is authenticated against enrollment scan and gains access to the network

Achieving strong authentication with OneSign is just that fast and easy.

In addition to supporting the easy integration of additional forms of authentication, OneSign offers these key benefits:

Non-intrusive

Organizations can implement OneSign without changing existing applications or modifying user logon behavior.

Plug and go installation

OneSign is packaged in a secure, 1U rack-mounted device (with redundant unit) that requires nothing extra to buy or install.

Password policy support

Customers can configure support for unique passwords and change passwords automatically in the background.

Security policy support

Enterprises can assign different security policies to different users or groups of users.

Shared credentials support

Customers can organize applications into groups that share a common credential store.

Shared workstation support

Multiple users can sign on to a shared workstation without logging out of the desktop.

Client-side logging

Security officials can monitor application or access logs to determine which user is accessing what application and when.

Self-updating agent

This feature simplifies deployments and updates without additional administrative overhead.

Business process integration

Custom operational workflows can be integrated with SSO deployments. Examples include — personalized messages, mapping user hard drives to workstations, delivering dynamic roaming sessions, etc.

What customers say about strong authentication with OneSign

Here's how one OneSign customer described his organization's experience deploying strong authentication with ESSO:

> *"It was very easy to integrate OneSign with our biometric implementation for strong authentication. We set it up so that OneSign automatically changes the users' passwords behind the scenes. This increases security because the passwords are complex and up to 32 characters in length, far greater length than what we could ever ask our users to remember. Also, users will never actually know their passwords, thereby eliminating the possibility and the risks of sharing passwords."*
>
> — Steve Siress, Network Systems Manager,
> Enterprise Bank & Trust of
> St. Louis and Kansas City

A more secure future

Creating a strong authentication solution with Imprivata OneSign gives you an effective, easy, and affordable way to follow Gartner's recommendations to implement password management and utilize strong and two-factor authentication.

Looking ahead, as security needs increase, Imprivata OneSign customers have the assurance of knowing that their ESSO solution will be able to integrate a variety of authentication options as needed.

For more information on how you can easily deploy strong authentication with OneSign, please visit:

http://www.imprivata.com or contact Imprivata at **781-674-2700.**

10 Maguire Road
Building 2
Lexington, MA 02421
v 781 674 2700
f 781 674 2760

1.877.ONESIGN

Imprivata Europe
Forsyth House
77 Clarendon Road
Watford
Herts, WD17 1LE
United Kingdom
v+44 1923 813511
f+44 1923 813501

www.imprivata.com