imprivata®

A More Secure Front Door:

SSO and Strong Authentication

TABLE OF CONTENTS

INTRODUCTION

Times change. Sometimes they change even faster than we might expect, as recent developments in Strong Authentication have shown. Just a few years ago, the idea of requiring users to provide a second form of identity to gain access to IT resources was seen by many as only necessary for remote access security or top-secret jobs.

Not anymore. Today, companies of all types and sizes are deploying Strong Authentication inside the corporate firewall, enterprise-wide -- even within applications. Most regulatory bodies are mandating it, and an increasing number of organizations consider it an essential part of data security best practices. A recent report by the Commission on Cyber security for the 44th President recommends it for the government and consumer companies. As the global economic downturn results in unprecedented workforce reductions, the security risk of insider security breaches has never been greater. At the same time, Strong Authentication technologies have become more practical, affordable, easy, and flexible to implement.

For all of these reasons, there's never been a better time to take advantage of the increased data security of Strong Authentication. But what form(s) of Strong Authentication are best for you and your organization? What factors should you consider as you evaluate Strong Authentication? What capabilities do you require? What are the opportunities, issues, and trade-offs you can expect? Imprivata has published this white paper to help answer these and other key questions.

THE ADVANTAGES OF STRONG AUTHENTICATION

In a recent Forrester Research report, Analyst Bill Nagel stated that "MFA (multi-factor authentication) adoption is rising steadily, and even firms not in heavily regulated industries need to adopt." Imprivata's own 2009 survey of customers revealed that nearly 47% had already deployed Strong Authentication and another 45% were considering doing so.

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 will grow dramatically.

Increased awareness

The rising incidence of internal data breaches has alerted corporate executives of the real threats to their information assets — and the potentially grave consequences to their business operations, customer relations, and financial performance. For example:

- A senior financial analyst in the sub-prime lending division of Countrywide Financial stole and sold the Social Security numbers of as many as two million loan applicants over a two-year period.
- Former employees of Lending Tree participated in password sharing with other mortgage lenders, giving them access to the company's customer database which they used to market their own products and services.
- A former contractor to the State of Massachusetts gained access to a workers' compensation database and stole personal information for use in obtaining fraudulent credit cards
- A man who worked in the admissions office of Columbia Presbyterian Hospital/Weill Cornell Medical Center stole the Social Security numbers of 50,000 patients and sold them for illegal activities.
- A terminated Fannie Mae IT contractor used his network access to remotely plant a logic bomb that could have destroyed data on 4,000 servers had it been successful.

For each of these examples, there are many more that have not received media coverage or resulted in well-publicized legal action.

Increased regulation

Within the last decade, 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 loss of brand reputation resulting in negative customer reaction.

More choices

As demand for Strong Authentication has grown, so have the number and variety of commercially-available forms of Strong Authentication devices that organizations can deploy. This means organizations are in a better position to choose the types of Strong Authentication that make the best sense for their different user populations. For example, many healthcare workers need solutions that support their workflow with workstation sharing, rapid access, easy user authentication, and a way to handle unattended workstations. In contrast, financial services companies need strong authentication methods that make data security the highest priority, with convenience and speed of lesser concern. For most companies, the security benefits of strong authentication cannot come at the expense of employee productivity or customer service levels. In response to these diverse needs, the industry has developed a broad range of Strong Authentication devices, such as laptops with built-in fingerprint biometric swipes, keyboards with smart card readers, computers with built-in cameras, and laptops with integrated readers for facility access cards. As a result, organizations today are in a better position to find solutions that meet their unique security needs.

Greater affordability

As competition heats up and technologies advance, the cost of Strong Authentication devices has started to drop significantly, indicating a maturing market. For example, biometric fingerprint scanners were once bulky devices costing upwards of $100 to $200 each. Today, small, portable scanners of similar capability can be purchased for under $30. In addition, many manufacturers now produce keyboards, laptop computers, and even mobile phones with built-in biometric scanners at little incremental cost since there is little or no cost for packaging. Similarly, USB proximity card readers that sold for over $100 a few years ago are now selling for less than half that amount as sales volumes increase and the technology becomes commoditized.

Improved reliability

Technological advances have improved the performance and reliability of Strong Authentication technologies to the point that widespread deployment to large user populations is more feasible and manageable.

More applications

While Strong Authentication is still primarily used to confirm user identity before gaining network access, organizations have begun to employ it in other innovative ways. For example, some organizations now require user authentication for employees to access business-critical applications, or even when performing certain sensitive transactions. This is happening today in hospitals and pharmacies. As more records and transactions occur online, hospitals are becoming paperless – switching to fully electronic medical records (EMR). Many EMR solutions require prescribers to reconfirm their identities whenever they enter online prescriptions for patient medications. The same is true for many brokers and bankers, who must authenticate themselves before conducting key financial transactions.

Growing virtualization

More organizations are now moving from traditional distributed PC-oriented environments to the use of virtual servers and virtual desktops that can be accessed from almost anywhere. This new model effectively removes the links that associate a user with his or her workstation and its physical location, thereby challenging organizations to think in new ways about desktop security and the role of Strong Authentication. Business continuity and pandemic planning often dictate providing employees with IT access from outside the boundaries of the enterprise. It is best practice to use strong authentication to guarantee the identity of these remote users working offsite.

Analyst recommendations

Analysts are also leading the move to Strong Authentication. An August 2004 report by Gartner ("Assess Authentication Methods for Strong System Security") outlines two primary recommendations for increasing security and reducing password issues: 1) implement password management; and 2) utilize strong, two-factor authentication. More recently, a 2008 study by Aberdeen Group revealed that organizations enjoying best-in-class security performance had increased their usage of multi-factor Strong Authentication by 300% over a nine-month period. This suggests that the use of multiple factors will continue to gain momentum as a proven means of improving overall security.

Proven results

Above all, the most compelling reason for the growing adoption of Strong Authentication is that it works. According to that same Aberdeen Group study, organizations that have deployed Strong Authentication have realized significant decreases in the number of security-related incidents, the volume of authentication-related helpdesk calls, the costs of secure authentication management, and financial losses due to fraud. In particular, the study showed that organizations achieving Best-in-Class performance were able to reduce by more than one-half the amount of human error related to security, the number of incidents of non-compliance, and the total cost of addressing security incidents.

THE VALUE OF STRONG AUTHENTICATION

On the face of it, the logic for implementing strong, or two-factor, authentication 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 Authentication. They include:

The elimination of passwords

The proliferation of application passwords in recent years has negatively affected productivity and data security in many organizations. Users have difficulty remembering multiple complex passwords and resort to either writing them down where they can be stolen, or calling IT helpdesks for frequent password resets. By deploying Strong Authentication, organizations can eliminate the need for users to deal with passwords entirely. This permanently solves a common user complaint while reducing resource requirements at IT helpdesks and strengthening security, enterprise-wide.

A fast ROI

With the cost of authentication technologies dropping, Strong Authentication has been proven to not only improve security, but also lower helpdesk and security management costs. Experts believe there are several reasons for this. First, use of Strong Authentication is easier for users than memorizing complex passwords, so they make fewer helpdesk calls for password resets. Strong Authentication also has a definite deterrent effect against potential insider threats, resulting in fewer incidents and thus, lower security management costs.

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 the proper management, tracking and reporting functionality -- provides demonstrable compliance in the form of audit logs that record all relevant access activity.

Stronger application and transaction-level security

Today, more organizations and industries are relying on online records and transactions to be more productive, reduce paperwork, and support environmental sustainability. As more business tasks are performed within an online environment, organizations have an opportunity to apply additional security measures at both the application and transaction levels. Strong Authentication gives organizations a powerful tool to selectively deploy an additional level of security at points where it can be most effective. For example, there are companies now requiring users to authenticate their identities before accessing critical enterprise applications, such as financial or manufacturing systems. Others are mandating Strong Authentication before a user can perform sensitive transactions, such as electronic funds transfers.

LEADING AUTHENTICATION METHODS

As the demand for stronger authentication measures has grown, so have the solutions available to organizations. The following are the most prevalent 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 are often too complex for users themselves to remember, resulting in an upsurge of costly calls to helpdesks for assistance. This, in turn, has a negative impact on productivity as users 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. In environments such as healthcare, where a clinician has to enter the same logon credentials with each different patient visit, the amount of time spent on this repetitive, unproductive task can be significant.

ID tokens

ID tokens are small devices which generate numeric codes that validate user 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 One-Time Password (OTP) for two-factor authentication. Leading ID token vendors include RSA, Secure Computing and Vasco. Traditionally, tokens have been used for employees accessing networks, and applications via remote access. There are many forms of tokens, including time-based and event-based tokens. Time-based tokens generate OTPs based on a combination of a secret key and current time, while event-based tokens generate OTPs by the press of a button on the device.

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, PKI credential store, and application password provider. Frequently, companies issue smart cards so they can be used not only for access control, but also to digitally sign e-mails, files or content to prove their authenticity. 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 powers up the card and reads back 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 also used as building access cards. Passive proximity cards are offered by companies such as HID, Axalto, and Gemplus, among others.

Active Proximity Cards

Active proximity cards include a wireless radio transmitter (worn by the user) that stays in constant communication with a receiver 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.

Biometrics

Biometric devices authenticate users with something that is uniquely theirs — facial features, fingerprints, hand geometry, or even their irises. Fingerprint biometrics are most commonly used, due to their reliability, affordability, and availability. 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 the user logs in, the device scans the fingertip and compares it to the data on file to complete the authentication process. Finger biometric devices are offered by companies such as UPEK and Authentec and are appearing in a growing range of forms, from scanners and area readers to USB devices, and built into laptops, PCs, and mobile phones. As the reliability of these devices increases and their cost declines, more organizations are expected to adopt finger biometrics as an effective, affordable, and easy-to-use form of Strong Authentication.

There are two common modes of fingerprint authentication. The first is Fingerprint Verification, which matches the fingerprint to the user after the user has provided a username, thereby establishing a one-to-one match. The second mode, Fingerprint Identification, tends to be more appealing to users because of its simplicity. The user presents a finger and is authenticated, which is considered a one-to-many match. Fingerprint Identification offers a much more streamlined workflow for the user and is generally better received.

All of the biometric 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, ease of implementation and acceptance, 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 or methods that will work best for you.

CONSIDERING ENVIRONMENT AND WORKFLOW

Every organization wants to prevent unauthorized access to its information assets — and all organizations can benefit from the use of Strong Authentication. Because organizations' environments and regulatory and workflow requirements vary greatly, different authentication technologies and procedures may be called for. For example:

- In a healthcare environment with strict requirements for tracking pharmaceutical orders, clinicians submitting orders electronically are required to confirm their identity to reduce the potential for fraudulent orders. When a clinician fills out the medication order form, the system prompts her to scan her fingerprint to validate that a) she is the same person currently logged into the application, and b) she is really who she claims to be. Upon successful re-authentication, the order is accepted and processed by the system.

- A behavioral health office with shared workstations needs to comply with the patient information confidentiality requirements of the Health Insurance Portability and Accountability Act (HIPAA). Therefore, its clinicians use proximity cards and a solution that allows them to authenticate themselves quickly -- and terminate sessions promptly -- at that shared workstation.

- A customer call center needs to meet PCI or customer privacy requirements for controlling access to the application and/or specific screens so only the appropriate personnel can view the information, and all access activities are tracked for auditability. Within a logged-in application, when a screen with private customer information is about to be displayed, the system prompts the user to re-authenticate to ensure that the same authorized person is reviewing the information.

- Other factors to consider include: the number of enterprise locations, the variety of roles and access requirements, and the use of remote access by traveling employees. The proper combination of Strong Authentication technologies can accommodate these and many other unique requirements.

CHOOSING STRONG AUTHENTICATION METHODS: 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? Are multiple servers or databases required to set up the solution? If using multiple authentication methods, what are the set up requirements to make them all work? Will end users be burdened if changes are made after devices are deployed? Is there an easy way to track access events, regardless of devices used? Can it be used as a deterrent?

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? Will users be concerned about privacy?

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 and supplying reporting facilities that support auditing requirements and objectively and easily prove compliance?

Industry-specific benefits

Are there aspects of the authentication method that make it better suited for certain industries or functional areas? For example, if employees have to wear gloves to do their jobs, then biometrics is not the choice for the organization.

Initial purchase cost

Is the cost of the authentication method worth the resulting improvement in enterprise security? Is there a cost per user that will grow every time a new user is added? What is the replacement cost – both for the device and its associated administrative burden – for the forms of Strong Authentication?

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?

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

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	$	$$
ID Token	Medium	Medium[1]	High	$$$	$$$
Smart Card and USB Token	Low	Medium[1]	High	$$$	$$$
Passive Proximity	High	High[1]	High[2]	$$	$
Active Proximity	Medium	High[3]	Low	$$$$	$$
Finger Biometrics	High	High	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. When combined with another authentication factor
3. 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, finger biometrics 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, 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.
- If you want to repurpose existing technology then enabling building access or identity cards might be most efficient.

SPECIFIC CONSIDERATIONS

Even if you have decided which method of authentication is best for you and your organization, there are a number of other, more specific factors you should consider before you make your purchase decision, as they could affect the cost, resource requirements, and effectiveness of your solution. During the evaluation process, you should ask the following questions about every Strong Authentication solution on your short list:

1. How does the Strong Authentication solution integrate with your existing directory infrastructure?

The Strong Authentication system should not require changes to the existing directory infrastructure. Directories are the critical backbone for most IT organizations and keeping them reliable means keeping them as close to their core functionality as possible. Layering additional schema changes or running application software on the directory should be avoided at all costs because of the potential to destabilize the overall system, especially if directory replication is involved.

2. How does the Strong Authentication solution affect your existing application infrastructure?

The Strong Authentication solution should not require any changes to the existing application infrastructure for Windows, Web or mainframe applications. It should also be able to integrate within applications to ensure strong authentication at the transaction level – for reauthentication, for example, immediately prior to performing a financial transaction or drug disbursement.

3. How does the Strong Authentication solution integrate into your existing environment?

The Strong Authentication solution should not require any programming in order to integrate into the application environment, or to handle any potential exception situations that could occur during deployment time to all client workstations. Adding Strong Authentication should also be a pure configuration activity – not a programming/scripting activity. Many strong authentication technologies are offered with an SDK to allow customized implementations. This should not be necessary in most situations.

4. How does the Strong Authentication solution handle disaster recovery and failover?

With the Strong Authentication solution responsible for managing all Windows authentications of all users in all systems of the enterprise, it is imperative that it provides out-of-the-box fault tolerance protection, preferably at the lowest possible level in order to avoid any potential end-user inconvenience. If possible strong authentication should continue to work in an off-line mode when the workstation is not connected to the network.

5. How and where are policies, credentials and logfiles of the Strong Authentication solution stored and made accessible for administrators?

The Strong Authentication solution should provide a secure transmission and storage facility for all security-sensitive data (e.g., policy information, credential information, logging information). This requires all data to be encrypted both in rest and in transit, without any configuration burdens to be imposed on the administrators of the Strong Authentication solution.

6. Can the Strong Authentication solution support the management of multiple Strong Authentication devices? Are there any additional costs/licenses required for specific authentication devices or combination of devices? Are there any additional server-side or client-side components that need to be configured or installed in order to support a specific strong authentication option?

Since the Strong Authentication solution will be replacing the current Windows authentication strategies, it is important that the single authentication action can be reinforced with a choice of strong, multi-factor authentication methods and technologies. These Strong Authentication options should also be available in both online and offline (disconnected from the network) modes.

7. Does the Strong Authentication solution provide any logging and/or reporting facilities? Are there any additional licenses required for this? Are there any server/client-side software components required for this?

The Strong Authentication solution should provide standardized reporting and notification capabilities that capture all authentication and password management related events that take place in the system. These reports and notifications should be available through an online Web interface, e-mail, and scheduled export mechanisms to remote reporting and archiving systems to ensure compliance requirements are easily met.

8. How does the Strong Authentication solution integrate with metadirectory and/or provisioning systems?

The Strong Authentication system should be able to support identity-standard provisioning systems, as well as any future implementations of SPML-based provisioning and metadirectory systems. This will ensure that when password changes are initiated in different backend systems, these changes will also immediately be made available in the Strong Authentication solution. This will also ensure ease of deprovisioning.

9. How does the Strong Authentication solution integrate existing physical access policies into its logical access policies?

The Strong Authentication system should provide facilities for location-based authentication, so that each user's location can be applied as a determining factor in the authentication policy. This enables an organization, for example, to grant access to an individual only after that user has badged into a specified company facility or secure area. The ability to apply network access policies that leverage location is extremely useful in situations where it is necessary to confirm that the properly authenticated user is accessing the computer from within a secure operational work area, such as a manufacturing control room or pharmacy area.

10. Does the Strong Authentication solution support fast user switching in thin and thick client architectures?

The Strong Authentication solution should provide support for different types of fast user switching to make the end-user experience of logging in and out as swift and convenient as possible. This means that: both thick clients and thin clients should support "kiosk-style" operation; both client-based and server-based computing environments should be supported; in server-based computing environments, both Citrix Presentation Manager and Windows Terminal Server environments should be supported; and in server-based computing environments, both roaming and concurrent sessions should be supported.

11. Can the Strong Authentication solution be extended to incorporate additional capabilities, such as Single Sign On?

As your IT security needs evolve, you may want to add more capabilities, such as Single Sign On. Your Strong Authentication solution should accommodate these and other capabilities easily. Single Sign On is an ideal complementary technology to deploy when Strong Authentication is being introduced by improving application-level password security and is often used to ensure further adoption of Strong Authentication policies.

MAKING STRONG AUTHENTICATION WORK FOR YOU

Whether you have already chosen and deployed a Strong Authentication solution or you're still in the evaluation process, you need a solution you and your organization can live with. As Strong Authentication becomes a part of your organization's daily life, you want it to be as user-friendly, easy to manage, and fully utilized as possible. The following questions and answers can help you get the most out of your Strong Authentication solution -- maximizing its effectiveness while keeping ongoing costs and administrative requirements to a minimum:

1. Should you have different Strong Authentication methods for different users?

It makes sense to match the method to users' roles, needs, and relative security risks. Other factors to consider include cost, workflow requirements, and ease of use.

2. Are there ways to streamline the administration of a Strong Authentication solution?

Administration can take many forms, including vendor-specific requirements, management tools, and user administration, and the tasks associated with them vary according to the organization's needs and preferences. However, there are some tasks that are necessary to achieve maximum benefit from the authentication choice, such as tracking and reporting. It's also a good idea to offload as much of the administrative burden as possible from users, because their ability to simply "plug and go" will help ensure organization-wide acceptance.

3. How can the use of Strong Authentication be made as easy as possible for users?

The key is to choose solutions that are both secure and easily adopted by end users. It is important to gain user acceptance of the type of Strong Authentication before making a purchase by consulting with them on the options and their preferences. In general, users will welcome a solution that does not require them to alter or abandon their established routines. For example, in environments where a user is required to carry a badge to gain entry into doors, reusing that same device for desktop access can be easily accepted.

4. Once users are authenticated, how do we more effectively address security when users walk away from their computers?

There are many solutions to this issue, but most have been ineffective. Many organizations require a locked screen saver or inactivity timeout to address the walk away security issue, but these are easily defeated by just moving the mouse. Imprivata is addressing this problem with a unique new solution, OneSign Secure Walk-Away. It uses a combination of active presence detection and facial biometrics to automatically lock a workstation upon user departure, and then automatically unlock it when the same user returns. OneSign Secure Walk-Away is the only solution to effectively address this issue today.

5. What is the best way to deploy Strong Authentication at multiple locations?

When choosing a device solution, make sure it meets both the security needs of the business and the convenience needs of the users. When choosing a management system for your devices, pick one that is geographically scalable and can support a range of Strong Authentication options. This way, you can be confident in the ability of the system to scale, as well as to address the needs of various departments within the organization, which many times have different requirements for Strong Authentication. Be sure to follow the vendor's list of best practices to ensure your final outcome will be optimized.

BEYOND STRONG AUTHENTICATION

Today, you may regard Strong Authentication as a "one-off" solution that fulfills your most critical needs for enterprise access security. However, it's important to know that your Strong Authentication solution can provide even greater value going forward, acting as a platform for deploying additional capabilities across your organization to further strengthen security, satisfy related user needs, and reduce costs.

Strong Authentication and Single Sign-On

Single Sign-On enables your user community to logon to the network and sign on to all the applications they are authorized to use on a daily basis by using a single strong password. Single Sign-On relieves users of the burden of memorizing multiple passwords, increases productivity by helping users avoid getting locked out of systems, and lowers resource costs by reducing the number of password reset calls to your helpdesk. Above all, Single Sign-On strengthens IT security because users no longer resort to writing down passwords and leaving them where they can be stolen and used by unauthorized people.

Combining Strong Authentication with Single Sign-On gives your organization proven security benefits, as recommended by leading analysts and security experts. At the same time, the combination of both solutions enables you to enforce strong security policies enterprise-wide while increasing user satisfaction and requiring no disruptive changes to user workflow or behavior.

Strong Authentication and Integrated Physical/Logical Security

In most organizations, physical security (systems that control physical access to buildings and work areas) and logical security (systems that control access to IT resources) are separate realms. This lack of integration between physical and logical security systems creates gaps that can be exploited and prevents centralized management and control of overall security. In many cases, for example, a terminated employee may be immediately barred from re-entering corporate facilities, but may still be able to gain remote access to the corporate network for days or weeks before privileges are revoked. An integrated physical/logical security solution makes it possible to link both security environments, synchronize control and response.

THE IMPRIVATA ONESIGN® SOLUTION FOR STRONG AUTHENTICATION

Imprivata OneSign® Authentication Management is a unique user authentication solution that integrates a broad range of flexible and powerful strong authentication types – all managed from within a single administrator framework. OneSign eases the cost and complexity of managing independent systems and provides a central location for reporting access events across all Strong Authentication devices, strengthening security while reducing the burden of regulatory compliance.

Flexible authentication options

OneSign Authentication Management provides native support for a broad range of plug-and-play authentication options such as One-Time-Password (OTP) tokens (including built-in control and management support for VASCO® DIGIPASS®) finger biometrics, smart cards, proximity cards, building access cards, and USB tokens. Simply plug them into your workstation and you are ready to go.

Consolidated reporting

With OneSign Authentication Management, you can easily report in real-time an aggregated view of when, how and from where an employee gained access to the network. By having all access information available at the push of a button via standardized reporting, OneSign Authentication Management provides critical value in helping you rapidly respond to audit inquiries that may otherwise require manual viewing and collation of independent system logs. When adding OneSign Single Sign-On, you can also incorporate reporting on user access events to applications as well.

ROI right out of the box

The power of OneSign Authentication Management is that it comes packaged in a hardened appliance. OneSign Authentication Management is designed to be affordable and easy to adopt. Purpose-built for flexible and rapid enterprise deployment, OneSign's appliance-based approach to user authentication dramatically minimizes implementation time, infrastructure needs, and installation costs – accelerating your return on investment right out of the box.

Application Transaction Level Strong Authentication

The Imprivata OneSign ProveID capability allows an application to leverage OneSign's strong authentication services to positively identify a user at any point in the application workflow. Examples of ProveID in use include banking environments where positive identification of a user is required prior to executing a financial transaction, and healthcare environments where positive identification of a user is required at the point of drug disbursement.

Built-in RADIUS Host for Remote Access Authentication

OneSign Authentication Management contains a built-in RADIUS host for handling remote access authentication using VASCO DIGIPASS tokens, SecurID, Secure Computing tokens or domain passwords.

OneSign Authentication Management can also be purchased alone or as part of The OneSign Platform™, the technology solution that is helping more than 800 companies around the globe to achieve their most pressing Employee Access Management security mandates.

WHAT CUSTOMERS SAY ABOUT STRONG AUTHENTICATION WITH IMPRIVATA ONESIGN

Here's how OneSign customers describe their experiences deploying Strong Authentication:

"Among its many benefits, Imprivata supports multiple strong authentication methods. In fact, organizations can even use it with multiple, interchangeable methods, making it an extremely flexible solution."

-- Rifat Ikram, Vice President of Electronic Delivery and Support Services, Justice Federal Credit Union

"Staff carry their HID physical access cards with them already, so using these cards for network access as well made a lot of sense. We can re-use our existing systems to provide additional value, while also providing staff with a system that suits their individual needs. Imprivata OneSign makes it all possible."

–Dr. Zafar Chaudry, Director of Information Management and Technology, Liverpool Women's NHS Trust

"Once they have the convenience of SSO and strong authentication for access to critical applications, department heads will want every user enabled for every application."

–Bill McQuaid, AVP and CIO Parkview Adventist Medical Center

"All our employees – whether loan officers, customer service reps, or IT– are more productive. We've eliminated 95% or more of password-related reset calls."

-- Rifat Ikram, Vice President of Electronic Delivery and Support Services, Justice Federal Credit Union

A MORE SECURE TODAY -- AND TOMORROW

Creating a Strong Authentication solution with Imprivata OneSign gives you an effective and affordable way to implement the security measures highly recommended or mandated by regulatory bodies, industry analysts, industry associations, and governmental commissions.

At the same time, OneSign gives you the flexibility to choose the right combination of Strong Authentication methods that best suits your business, your organization, and your employees' different roles and responsibilities -- no matter how large or geographically-dispersed your enterprise.

Above all, OneSign is a solution your organization can live with -- because it requires little from users to maintain compliance, and because it actually enhances their productivity by reducing password problems and help desk calls.

For more information on how you can easily deploy Strong Authentication with OneSign, please visit: http://www.imprivata.com/onesign_authentication_management or contact Imprivata at 1-800-ONESIGN or 1-781-674-2700.