

Facility Access and Computer Access Converge:

Computer logon with facility access card makes sense, both in terms of security and convenience.

Today, most facility access cards are used only for physical access. As customers begin to demand more capabilities from their facility access cards, the industry is responding by offering easy and effective add-ons that leverage the card's value to the customer.

The most frequently requested add-on is the ability to use the facility access card for computer logon. Network industry professionals agree that the familiar form factor of the ID card makes it the multi-purpose venue of choice. The question is, how does this approach work, and how does it stack up against other logon security technologies?

In fact, when a standard facility access card is combined with a high-quality logon management software, it provides two-factor authentication, and the ability to easily use strong complex passwords for all logon locations. This achieves the high level of logon security that network industry professionals recommend should be implemented, or at least planned for, by all organizations.

Further, facility access cards are currently available in a wide spectrum of card technologies that also fit the advanced security requirements of more security-sensitive organizations:

- To add an additional layer of security, organizations can opt for the newest contactless facility access cards, which are protected by an internal card PIN and encryption keys, and can carry several kBytes of sensitive user data.
- Organizations that want to have a more powerful microprocessor on their card to perform complex security operations, such as support for PKI functions, can choose the newest contactless cards based on dual-interface smart chips, or opt to embed a contact chip on their facility access card.

This paper first addresses the "password problem", which is implicit in the logon process, then provides a direct comparison between a logon management solution based on a facility access card, and other available logon security technologies. It concludes that, with the many advantages offered by the logon management software and the wide spectrum of cards available, the facility access card is well positioned to provide the ideal computer access protection for the majority of companies and institutions.



The Password Problem: Why the logon process makes many companies vulnerable

The timing is ripe for the facility access card to be used for computer logon. Many companies are at risk, simply because of the nature of passwords. Passwords are effective vehicles for protection of computer access, but only when they are correctly used. Unfortunately, it is generally acknowledged that passwords are used incorrectly more often than correctly, simply because passwords are difficult to remember.

A few years ago, many of us had only one password to remember. Today, most people have a few passwords to remember, and many of us have dozens. On top of this, "best security practice" requires that we change our passwords frequently and use long, complex passwords. To use passwords effectively - so that they protect the way that they should - a logon management solution is required.

Technology Comparison Tables

There are various vehicles for solving the "password problem", with varying degrees of complexity, to suit the specific needs of different companies and institutions. The following pages show a side-by-side comparison of the general characteristics and security considerations of four logon security technologies.

Alongside the One-time Password (OTP), Certificate-based Logon (PKI), and facility access card-based logon management solution, which are based on tokens or cards, we have also included server-based Single Sign-on (SSO) in our comparison, since SSO systems must rely on secure user authentication and are often combined with card or token-based two-factor authentication systems. Biometric authentication has not been included in the comparison tables, since it is not directly comparable to the listed methods, however a note about this technology has been included on the last page of this paper.

Note that in this comparison, the "facility access card logon" description assumes the incorporation of a high-quality logon management software that is capable of working "out-of-the-box" with a diversity of card technologies, including today's 125kHz and 13.56 MHz contactless cards as well as contactless cards with embedded contact chips. When a specific technical approach is cited, the Sphinx Logon Manager software is used as the basis for comparison. Other logon management products may differ in their approach.

The different aspects of each technology are discussed under the following headings:

General Overview

Logon Security Comparison

Background System Considerations

End-user System Considerations

Bottom Line

General Overview

	One-time Password (OTP)	Certificate-based Logon (PKI)	Single Sign-on (SSO)	Facility Access Card Logon* i.e., Sphinx Logon Manager
Purpose	<ul style="list-style-type: none"> Increases logon security at point of entry into a network. 	<ul style="list-style-type: none"> Increases logon security at point of entry into a network. Provides support for additional certificate based functions, such as email encryption and digital signatures for documents. 	<ul style="list-style-type: none"> Adds ease-of-use and unified logon security for applications that have been integrated with the single sign-on product. (Does not impact logon security at point of entry into network.) 	<ul style="list-style-type: none"> Increases logon security at point of entry into a network. Increases logon security at all other website and application logon locations. Adds ease-of-use by recording logon data, and executing logon automatically.
Short description	<p>End-user has a battery powered token that has a microprocessor and a digital display. Upon pressing a button on the token, display shows a numeric code that the token generates based on a secret key, and an event or time counter.</p> <p>To logon to a network, user types in the current code number from the token display and his PIN. A token authentication server verifies the entered code and PIN and grants or denies access.</p>	<p>End-user has a card or token that has cryptographic processing functionality. Card stores a digital certificate (which contains the public key) and the associated private key, which are accessed during the authentication process with an authentication server.</p> <p>To logon to a network, user inserts token into USB port or reader and types his PIN. Entry of the correct PIN opens the token so that the logon process can access the token's digital certificates and cryptographic functions. A certificate authentication server communicates directly with the card to verify that the user certificate and its associated private key are authentic, and grants or denies access.</p> <p>Additional notable logon-related features:</p> <ul style="list-style-type: none"> Pulling card from card reader logs off end-user, or locks computer. Configurable per computer. 	<p>For the purposes of this comparison, single sign-on applications are defined as administrator controlled server-based systems that allow an end-user to access multiple applications within a corporate environment without having to logon to each application individually.</p> <p>Since SSO-integrated applications are protected only by a single logon process, they are typically paired with a form of improved authentication security at the point of entry (i.e. Active Directory), such as two-factor authentication. After user has successfully completed initial authentication, user automatically has access to all integrated applications for which he has been granted permission by the administrator.</p>	<p>End-user has facility access card. To logon to a network, user presents card to card reader and types PIN. Entry of the correct PIN opens the card (or card server account for proximity cards) so that the logon process can access the user name and password information.</p> <p>In its standard configuration, this "out-of-the-box" facility access card logon allows user to access multiple networks (no PKI required), websites and applications by clicking on an entry from within the logon manager software. Facility access card logon can also optionally be used within a PKI environment, where it can support the full spectrum of certificate-based functions.</p> <p>For the purposes of this comparison, the facility access card logon description assumes the incorporation of a high-quality logon management software that is compatible with a wide range of facility access cards, both contactless cards, and cards embedded with a contact chip.</p> <p>Additional notable logon-related features:</p> <ul style="list-style-type: none"> Pulling card from card reader logs off end-user, locks computer, or shuts down computer. Configurable per end-user card. Software auto-records and auto-fills logon data for websites and applications, and saves address and payment information for use in websites and applications.

* In "Facility Access Card Logon" column: when a specific technical approach is cited, it refers to the Sphinx Logon Manager software product. Note that other logon management products may differ in their approach.

Logon Security Comparison

	One-time Password (OTP)	Certificate-based Logon (PKI)	Single Sign-on (SSO)	Facility Access Card Logon* i.e., Sphinx Logon Manager
User authentication	Two factor. Token code plus PIN.	Two factor. Token or card plus PIN.	NA. (Dependent on authentication method used at point of entry.)	Two factor. Card plus PIN.
Logon security at point of entry into network (i.e., logon to Windows)	<p>Strong.</p> <ul style="list-style-type: none"> Typically, the OTP solution gets the Windows password from the authentication server (or a local cache) and passes it to the Windows logon process via the Microsoft GINA API on the end-user's computer. Windows authentication process continues unchanged using the Kerberos v5 authentication protocol for domain and local access. Authentication process secured by symmetric keys. The keys are protected from unauthorized access by the token's internal security features. Continuously changing code displayed on token is generated based on time or events, to protect against replay attacks. 	<p>Very strong.</p> <ul style="list-style-type: none"> The Microsoft logon process uses the Kerberos v5 with PKINIT authentication protocol for domain and local access. The Microsoft GINA has built-in support for this functionality for Windows 2000 or higher. Process is secured by public/private key pairs, which are generated by and stored on the card chip. The private keys are protected from unauthorized access by the card's chip security features. The certificates used within the PKI system serve as the vehicles for the exchange of public keys. They contain the end-user's identification information, public key, and are digitally signed by a trusted authority so that the information cannot be changed without invalidating them. 	<p>Not applicable.</p>	<p>Strong.</p> <ul style="list-style-type: none"> Logon manager software reads user name, password, domain from card (or card server for proximity cards) and passes this data to the Windows logon process on the end-user's computer, via the Microsoft GINA API. Does not replace or change Microsoft GINA; only interacts with relevant functions. Windows authentication process continues unchanged using the Kerberos v5 authentication protocol for domain and local access. Authentication data secured by card-specific Triple-DES symmetric keys. Data and keys are additionally protected against unauthorized access by card's internal security features, including cards that are protected by an internal card PIN, and cards with data encryption capability. User can specify, securely store, and transfer strong, cryptic passwords directly into the logon process. When password policy is enforced, requires a specified password quality and regular password changes.
Additional logon locations that can be secured by this method	<p>Limited.</p> <p>Only secures additional logon locations of systems that have been integrated with, and are secured by, the token authentication server.</p>	<p>Limited.</p> <p>Only secures additional logon locations of systems that have been integrated with certificate-based authentication process.</p>	<p>Limited.</p> <p>Only secures additional logon locations of applications that have been integrated with single-sign-on system.</p>	<p>Unlimited.</p> <p>End-user stores logon information with card as desired, so additional logon locations can be secured at any time. No administrator integration required.</p>

Background System Considerations

	One-time Password (OTP)	Certificate-based Logon (PKI)	Single Sign-on (SSO)	Facility Access Card Logon* i.e., Sphinx Logon Manager
Impact on existing network infrastructure	Moderately high. Must be integrated to work with existing authentication systems.	High. Must be integrated to work with existing authentication systems, and throughout background system.	High. Must be integrated with all linked applications.	None.
Impact on ID card infrastructure	Requires additional token for logical access.	Contact chip can be embedded on facility access card.	None. (Unless used with an additional token to enhance security at the point of entry.)	Works with contactless facility access card, or contact chip embedded on card.
Background system components	<ul style="list-style-type: none"> ▪ Token authentication software is installed on a server computer. ▪ Key generation hardware may additionally be required. 	<ul style="list-style-type: none"> ▪ Certification authority (CA) and PKI components for certificate-based user authentication are installed on background system. ▪ Key generation hardware and certificate management system may additionally be required. 	<ul style="list-style-type: none"> ▪ Single-Sign-On (SSO) software is installed on a server computer. ▪ Software connectors (scripts and agents) installed and integrated for each logon application on server computer. 	<ul style="list-style-type: none"> ▪ Optional: card management software installed on a server computer.
Complexity of background system setup and maintenance	<p>Moderately high.</p> <p>Company must make a commitment to integrate with background system:</p> <ul style="list-style-type: none"> ▪ The token authentication server must be integrated with the end-user authentication system in use (for example, Windows Active Directory). ▪ In order to protect additional applications, the respective server application must also be integrated with the token authentication server, or a token-protected SSO. 	<p>High.</p> <p>Company must make a commitment to integrate with background system:</p> <ul style="list-style-type: none"> ▪ Public Key network infrastructure must be carefully planned before implementation begins. ▪ Then, PKI environment is configured, certification paths and trust relationships are established, and user authentication server is configured for certificate-based logon. ▪ Certificates are issued and managed for each user card or token. ▪ Any new PKI-aware applications must be integrated as required. ▪ Public Key Infrastructure (PKI) must be maintained to adapt to changes in the IT infrastructure. 	<p>High.</p> <p>Company must make a commitment to integrate with background system:</p> <ul style="list-style-type: none"> ▪ Single-sign-on software must be integrated with the existing IT infrastructure. ▪ Trust relationships are established and SSO agents are installed with all application servers that need to be accessible through SSO. ▪ Access rights are configured and maintained for individual users and/or groups. ▪ User access rights must be administrated and application interfaces configured whenever applications are added or upgraded, or when users and group associations change. 	<p>Low.</p> <ul style="list-style-type: none"> ▪ Software is an out-of-the box setup. No integration required. ▪ When used with the optional server: because software works with standard Windows server technology and client and server communicate over standard IP channels, only a few server settings need to be specified. System is ready for use within a few minutes. ▪ No integration with existing end-user authentication system or other applications required.

End-user System Considerations

	One-time Password (OTP)	Certificate-based Logon (PKI)	Single Sign-on (SSO)	Facility Access Card Logon* i.e., Sphinx Logon Manager
End-user system components	<p>Software:</p> <ul style="list-style-type: none"> OTP token client installed on end-user computers. Optional configuration tools may also be installed to allow the end-user to perform certain token management functions like changing the PIN. <p>Hardware:</p> <ul style="list-style-type: none"> Token with display required for each end-user. (Note that this must be maintained separately from facility access / ID card and a picture and employee ID # cannot typically be printed on this token.) 	<p>Software:</p> <ul style="list-style-type: none"> Card-specific Crypto Service Provider (CSP) software installed on each end-user computer. <p>Hardware:</p> <ul style="list-style-type: none"> Smart cards or tokens are issued to end-users. Contact smart card or USB token reader installed at each end-user computer. 	<p>None. (Unless used with an additional token to enhance security at the point of entry.)</p>	<p>Software:</p> <ul style="list-style-type: none"> Logon manager software installed on each end-user computer. <p>Hardware:</p> <ul style="list-style-type: none"> Facility access cards with or without contact chip are issued to end-users. Desktop card reader installed at each end-user computer.
Lifespan and durability	<ul style="list-style-type: none"> OTP tokens often have a limited lifespan due to an expiration date or limited battery life. Since most OTP tokens have displays and buttons, they are inherently more sensitive to water or harsh environments. 	<ul style="list-style-type: none"> While sturdier than an OTP token, a contact chip card is still vulnerable to physical damage (bending of card, module scratching in reader) or contamination by liquids. 	<p>NA.</p>	<ul style="list-style-type: none"> Contactless cards and readers are extremely durable and have a long lifespan. When a contact chip is embedded on a facility access card: while sturdier than an OTP token, a contact chip card is still vulnerable to physical damage (bending of card, module scratching in reader) or contamination by liquids.
Ease of use	<ul style="list-style-type: none"> Manual entry of code from display is cumbersome and error-prone for end-user. 	<ul style="list-style-type: none"> User inserts token or card and enters PIN for authentication. 	<ul style="list-style-type: none"> Applications that have been integrated with SSO product are immediately accessible, with no need to logon. 	<ul style="list-style-type: none"> User inserts card and enters PIN for authentication. Software auto-records and auto-fills logon information.
Productivity enhancement	<p>Low.</p> <p>Impacts only initial point-of-entry.</p>	<p>Low.</p> <p>Impacts only initial point-of-entry.</p>	<p>Moderate.</p> <p>Impacts only integrated applications.</p>	<p>High.</p> <p>Enhances productivity for all logon locations.</p>

Bottom Line

The table below provides a summary of the approximate relative total cost of ownership that can be expected with each solution.

	One-time Password (OTP)	Certificate-based Logon (PKI)	Single Sign-on (SSO)	Facility Access Card Logon* i.e., Sphinx Logon Manager
Acquisition cost	++++ OTP token systems are proprietary and often costly.	+++ PKI background administration systems can be costly and complex.	++ Most solutions need agents or connectors for each application. Full acquisition cost consists of licensing price plus cost of required standard or custom-programmed connectors.	++ No added card costs for facility access card installations.
Integration and deployment cost	+++ Requires integration with existing authentication system.	+++++ Establishing PKI environment must be well planned and can be a lengthy process (CA, trust relationships, Certificate Enrollment Agents, Certificate Revocation Lists...).	++++ Requires establishing interfaces with all integrated applications. Integration of SSO systems with diverse legacy infrastructure can be time consuming and costly.	+ No change to network. No integration of background system required.
Operating cost	++++ Token expiration / replacement cost, maintenance of background authentication system.	+++ Maintenance of complex PKI environment.	+++ Maintenance of background authentication interfaces.	+ No background interfaces to maintain.
Total cost of ownership	+11	+11	+9	+4

Who might typically use this approach?	<ul style="list-style-type: none"> ▪ Larger institutions that are willing to commit to the integration effort with their background system. ▪ Institutions that use multiple platforms and legacy systems. 	<ul style="list-style-type: none"> ▪ Institutions that require a high level of privacy and have the IT resources to set up and manage this solution. ▪ Institutions that commit to a Public Key Infrastructure (PKI) typically also use it for email encryption and document signing. 	<ul style="list-style-type: none"> ▪ Larger institutions that have integrated applications, and are willing and able to maintain application links for their end-users. 	<ul style="list-style-type: none"> ▪ Can be used in any organization, since passwords are still the standard means of controlling access to networks and applications. ▪ Can also be used to enhance any of the other methods listed, to provide card-enabled logon to applications the other methods do not cover.
--	--	---	--	---

Summary: How Facility Access Card Logon Compares

This section summarizes how facility access card logon solutions compare overall to the other listed technologies in terms of logon security, solving the password problem, and infrastructure considerations.

Logon Security

All of the solutions discussed that provide "logon security at point of entry into network" use two-factor authentication - "what you have" (the token or card) and "what you know" (the PIN) - which means that they all provide strong protection for the network logon process. These include the One-time Password (OTP), Certificate-based Logon (PKI), and facility access card logon.

For Microsoft Windows environments, each of the network logon approaches relies on the security of the Windows logon process. Then, in association with a complex infrastructure, both the OTP and the PKI logon add another layer to the Windows logon authentication process. The facility access card logon approach accomplishes secure logon to Windows as well, but does not require an infrastructure change.

With respect to certificate-based logon, it should be noted that using a facility access card for computer logon works equally well in a PKI environment. Facility access card logon solutions such as the Sphinx Logon Manager offer a built-in PKI card interface option. Embedding a contact chip onto a facility access card makes it capable of supporting PKI-based applications, and the newest contactless cards based on dual-interface smart chips can also be used with both PKI environments and facility access solutions.

The single sign-on solution (SSO) can only be compared to the facility access card logon solution outside of the network logon arena, since it does not provide network logon. The advantage of the SSO - that the end-user doesn't need to remember or enter logon information for integrated logon locations - can be directly compared to the facility access card logon's end-user-based automated logon functionality for websites and applications. The main differences of the SSO: logon is limited to only those applications that have been integrated by an administrator, it requires constant maintenance to keep it up-to-date with changing user applications, and it must necessarily rely on a separate secure network logon solution. In fact, for installations that already have a SSO solution in place, it would make sense to combine it with a facility access card logon solution, for the securing of the initial computer logon and logon to applications that have not been integrated with the SSO.

Solving the Password Problem

In terms of the password problem, the first three solutions offer logon only to those websites or applications that have been integrated with the respective product or technology. Hence, their ability to solve the password problem is limited.

The facility access card logon solution does not limit the logon locations that can be protected, since it can be used with any website or application without requiring integration. With this solution, administrators may have the option to preset logon information on the card, but the storage of credentials for additional logon locations can be initiated by the end-user at any

time. This can be a valuable point for many organizations to consider. How many end-users enter the same password at every logon location - because it is the only one that they can remember (the most common password downfall)? If this is the case, what are the chances that end-users are using this same password for the organization's network, or other sensitive logon locations?

When end-users are empowered to use long, complex passwords at all locations - comfortable that they do not need to remember them - they can be confident that by doing so, they contribute to the security of the company. Also important for the individual, this use of complex passwords is additionally effectively protecting the security of their own identity in an increasingly internet-centric world.

Infrastructure Considerations

The goal of many companies and institutions is to introduce a logon solution that solves the password problem, but does not affect existing infrastructures that already work well. This is where a self-contained facility access card logon solution also shines.

In contrast to many other methods, a self-contained, "end-user managed" logon solution does not require any change to the network or the Windows logon setup, which is a big consideration for many companies. Indeed, since the first two solution types listed are more complex with respect to their initial integration and ongoing maintenance, they are typically only considered by companies that can commit the required resources (i.e. large security-sensitive organizations).

In short, the facility access card logon solution does not change the way security is setup - it just makes logon processes much more secure and efficient, through two-factor authentication and high quality passwords. As mentioned, PKI - with its added infrastructure - is also an option with facility card logon, but not a necessity.

Another strong plus of the facility access card logon solution is its ability to work with facility access cards that are already in use. Other solutions may require that additional special-purpose tokens be issued, which requires the corresponding additional infrastructure for issuance and administration of these cards.

Conclusion

Companies that currently use a facility access card or are considering adding one can leverage that investment by additionally using that facility access card for computer logon. Stacked up against other computer access protection methods, this approach compares very favorably. The two-factor authentication and strong encryption ensures that logon data integrity is maintained and that only the end-user who owns the data will be able to access it. The easy implementation and the way it works within the existing infrastructure, make it convenient for any organization to use. The choice of advanced card technologies available today means it can suit the security needs of any type of organization, making it the best all-around choice.

Note on biometric authentication:

Biometric authentication is not covered in this side-by-side comparison, since this technology is mostly used in combination with one of the above-mentioned card or token-based authentication methods.

The safety of a biometric authentication system typically relies on the security provided by the selected microprocessor card. During enrollment, a biometric image (digital "footprint" of an iris-scan or a fingerprint...) is taken from a biometric scanning device (iris scanner, fingerprint reader...) and then stored on the card. During authentication, the biometric data received from a current scan is then compared against the image stored on the card. If the images match, access is granted. Use of biometric authentication is still mostly reserved for high-security applications, because of added infrastructure costs, the lower than 100% recognition rate, and privacy considerations.

With respect to our comparison of the authentication methods above, it can most easily be integrated with Certificate-based Logon (PKI) and facility access card-based logon, since today's state-of-the-art contact and contactless smart cards can support biometric images.



Open Domain Sphinx Solutions, Inc.
www.odsphinx.com

© 2005 Open Domain Sphinx Solutions, Inc. All rights reserved.

This White Paper is for informational purposes only. Open Domain Sphinx Solutions has provided the information contained herein to the best of its knowledge but cannot guarantee the accuracy of any information presented in this paper. Product or company names mentioned herein may be the trademarks of their respective owners.

OPEN DOMAIN SPHINX SOLUTIONS MAKES NO WARRANTIES, EXPRESS OR IMPLIED, IN THIS DOCUMENT.