

Security Technology Comparisons

Comparison Technologies:

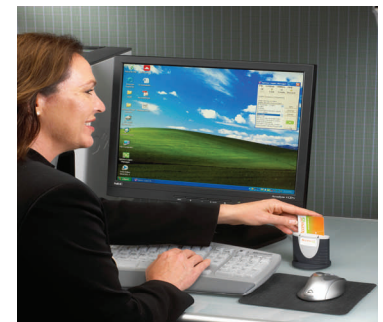
- One-Time Password (OTP)
- Certificate-based Logon (PKI),
- Server-based Single Sign-On (SSO)
- Smartcard-based password managers

Comparison Categories:

- General Overview
- Logon Security
- Background System
- End-user System
- Cost of Ownership

Today, IT managers have a host of security management technologies available to them. While all these products have their advantages, if the incorrect technology is chosen and the solution is too complex to manage, then the computer network and data may actually be less secure than before. IT may be lulled into a false sense of security when end-user compromises security with work-arounds designed for their convenience. Therefore, some of the key considerations before implementing any network security are:

- End-user's convenience
- Backend infrastructure modifications
- Value of the data being protected
- Ongoing support and maintenance
- Budget and
- Size of organization



Most high-quality logon management solutions provide at least two-factor authentication and the ability to easily use strong, complex passwords for all logon locations. This achieves the high level of logon secu-

urity that network industry professionals recommend. If the other identified concerns from above are not taken into consideration, the IT manager could open up a host of new problems and expenses.

This paper addresses the "password problem", which is paramount to the logon process, and compares different logon management solutions. Passwords are highly effective vehicles for ensuring authorized computer access, but only when they are correctly used. Unfortunately, end-users manage their passwords incorrectly by assigning simple passwords, writing down their passwords near their computers and repeatedly using the same password on other sites.

A few years ago, many of us had only a few passwords to remember. Today, we have dozens. It has become virtually impossible to use the Internet without passwords. On top of this, "best security practice" requires that we change passwords frequently and use long, complex passwords. Unfortunately, this has encouraged poor password management habits. To securely manage passwords effectively today, a logon management solution is required, but one that is also convenient, secure and portable for the end-user.

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 Smartcard-based Password Managers are One-Time Password (OTP), Certificate-based Logon (PKI), and server-based Single Sign-On (SSO) in our comparison. Biometric authentication was not been included in the comparison tables since it is an authentication factor that is often combined with one of the solutions listed above.



Security Technology Comparisons



General Overview

www.access-smart.com

Features	One-Time Password (OTP)	Certificate-based Logon (PKI)	Single Sign-On (SSO)	Smartcard-based Password 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	<ul style="list-style-type: none"> 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. To logon to a network, user types in the current code number from the token display and a PIN. The token authentication server verifies the entered code and PIN and grants or denies access. 	<ul style="list-style-type: none"> 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. To logon to a network, user inserts token into USB port or reader and types a 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. Additional notable logon-related features: <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> <ul style="list-style-type: none"> 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. 	<ul style="list-style-type: none"> To logon to a network, user presents card to card reader and types PIN. Entry of the correct PIN opens the card so that the logon process can access the user name and password information. 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. Additional notable logon-related features: <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 "Smartcard-based Password Manager" column: when a specific technical approach is cited, it refers to the Power LogOn Password Manager software product. Note that other logon management products may differ in their approach.

Security Technology Comparisons

Logon Security

Features	One-Time Password (OTP)	Certificate-based Logon (PKI)	Single Sign-On (SSO)	Smartcard-based Password Manager
User Authentication	<ul style="list-style-type: none"> Two factor. Token code plus PIN. 	<ul style="list-style-type: none"> Two factor. Token or card plus PIN. 	<ul style="list-style-type: none"> NA. (Dependent on authentication method used at point of entry.) 	<ul style="list-style-type: none"> Two factor. Token or card plus PIN.
Logon security at point of entry into network (i.e., logon to Windows)	<ul style="list-style-type: none"> Strong. 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. 	<ul style="list-style-type: none"> Very strong. 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. 	<ul style="list-style-type: none"> Not applicable. 	<ul style="list-style-type: none"> Strong. Logon manager software reads user name, password, domain from card 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	<ul style="list-style-type: none"> Limited. Only secures additional logon locations of systems that have been integrated with, and are secured by, the token authentication server. 	<ul style="list-style-type: none"> Limited. Only secures additional logon locations of systems that have been integrated with certificate-based authentication process. 	<ul style="list-style-type: none"> Limited. Only secures additional logon locations of applications that have been integrated with single-sign-on system. 	<ul style="list-style-type: none"> Unlimited. End-user stores logon information with card as desired, so additional logon locations can be secured at any time. No administrator integration required.

Security Technology Comparisons

Background System

Features	One-Time Password (OTP)	Certificate-based Logon (PKI)	Single Sign-On (SSO)	Smartcard-based Password Manager
Impact on existing network infrastructure	<ul style="list-style-type: none"> Moderately high. Must be integrated to work with existing authentication systems. 	<ul style="list-style-type: none"> High. Must be integrated to work with existing authentication systems, and throughout background system. 	<ul style="list-style-type: none"> High. Must be integrated with all linked applications. 	<ul style="list-style-type: none"> None.
Impact on ID card infrastructure	<ul style="list-style-type: none"> Requires additional token for logical access. 	<ul style="list-style-type: none"> Contact chip can be embedded on facility access card. 	<ul style="list-style-type: none"> None. (Unless used with an additional token to enhance security at the point of entry.) 	<ul style="list-style-type: none"> 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"> None. Optional: Card management software can be installed on a server computer.
Complexity of background system setup and maintenance	<ul style="list-style-type: none"> Moderately high. <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. 	<ul style="list-style-type: none"> High. <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. 	<ul style="list-style-type: none"> High. <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. 	<ul style="list-style-type: none"> Low. <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.

Security Technology Comparisons

End-user System Considerations

Features	One-Time Password (OTP)	Certificate-based Logon (PKI)	Single Sign-On (SSO)	Smartcard-based Password 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 card or token is issued to end-user. • Contact smart card or USB token reader installed at each end-user computer. 	<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 card or token is issued to end-user. • Contact smart card or USB token reader installed at each end-user computer. 	<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"> • Smart card or token is issued to end-user. • Contact smart card or USB token 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. 	<ul style="list-style-type: none"> • NA. 	<ul style="list-style-type: none"> • 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	<ul style="list-style-type: none"> • Low. • Impacts only initial point-of entry. 	<ul style="list-style-type: none"> • Low. • Impacts only initial point-of-entry. 	<ul style="list-style-type: none"> • Moderate. • Impacts only integrated applications. 	<ul style="list-style-type: none"> • High. • Enhances productivity for all logon locations.

Security Technology Comparisons

Cost of Ownership

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

Features	One-Time Password (OTP)	Certificate-based Logon (PKI)	Single Sign-On (SSO)	Smartcard-based Password Manager
Acquisition cost	<ul style="list-style-type: none"> • \$\$\$\$ • OTP token systems are proprietary and often costly. • Yearly subscriptions 	<ul style="list-style-type: none"> • \$\$\$\$ • PKI background administration systems can be costly and complex. • Yearly subscriptions 	<ul style="list-style-type: none"> • \$\$ • 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. 	<ul style="list-style-type: none"> • \$\$ • No added card costs for facility access card installations. • No subscriptions. • Use inexpensive smartcard chips
Integration and deployment cost	<ul style="list-style-type: none"> • \$\$\$ • Requires integration with existing authentication system. 	<ul style="list-style-type: none"> • \$\$\$\$ • Establishing PKI environment must be well planned and can be a lengthy process (CA, trust relationships, Certificate Enrollment Agents, Certificate Revocation Lists...). 	<ul style="list-style-type: none"> • \$\$\$\$ • Requires establishing interfaces with all integrated applications. • Integration of SSO systems with diverse legacy infrastructure can be time consuming and costly. 	<ul style="list-style-type: none"> • \$ • No change to network. • No integration of background system required.
Operating cost	<ul style="list-style-type: none"> • \$\$\$\$ • Token expiration / replacement cost, maintenance of background authentication system. 	<ul style="list-style-type: none"> • \$\$\$\$ • Maintenance of complex PKI environment. 	<ul style="list-style-type: none"> • \$\$\$ • Maintenance of background authentication interfaces. 	<ul style="list-style-type: none"> • \$ • No background interfaces to maintain. • Re-issue purchased licenses
Total cost	• 11 \$'s	• 12 \$'s	• 9 \$'s	• 4 \$'s

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 by any organization or individual, 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.
---	--	---	--	---

Security Technology Comparisons

Let's summarize how Smartcard-based Password Manager solutions compare overall to the other logical access 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 Smartcard 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 Smartcard-based Password Manager 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 Smartcard-based Password Manager logon approach accomplishes secure logon to Windows as well, but does not require any infrastructure change.

With respect to certificate-based logon, it should be noted that using a Smartcard-based Password Manager for computer logon works equally well in a PKI environment. Smartcard-based Password Manager logon solutions such as Power LogOn offer a built-in PKI card interface **option**. Embedding a contact chip onto a 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 Password Management solutions.

The Single Sign-On solution (SSO) can only be compared to the Smartcard-based Password Manager logon solution outside of the network logon arena, since SSO 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 Smartcard-based Password Manager logon's end-user-based automated logon functionality for websites and applications. The main differences are 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 Smartcard-based Password Manager 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 inability to solve the password dilemma. The Smartcard-based Password Manager solution, on the other hand, has no logon location limitations 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

Security Technology Comparisons

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)? How many end-users write passwords on notes by their computers (the second most common)? If this is the case, what are the chances that outsiders can easily capture a legitimate logon and access confidential data without the IT system administrator even detecting the intrusion? How could the IT system administrator know, the logon was legitimate?

When end-users are **empowered by their IT departments** to use long, complex passwords at all locations - comfortable that they do not need to remember them - they can conveniently access accounts and they contribute to the security of the network and ultimately the business. For the individual, this use of complex passwords is also 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 which solves the network security problem, is not a burden for their end-users and does not affect existing infrastructures that already work well. This is where a self-contained Smartcard-based Password Manager 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). Plus, since no infrastructure changes are required, a Smartcard-based Password Management solution is very portable onto other computer systems. Now the end-user can secure their home computer just as well as the office system, and a secure home system also protects the business system. In short, the Smartcard-based Password Manager solution does not change the way security is setup - it just makes logon processes much more convenient, secure and efficient through two-factor authentication and high quality passwords.

Another strong plus of the Smartcard-based Password Manager solution is its ability to work with facility access cards that are already in use. The Smartcard-based Password Manager can be combined with photo ID, magnetic stripe and RFID facility access. This allows companies to issue and manage a single card. Other solutions may require additional special purpose Smartcards 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 adding Smartcard-based Password Manager for computer and network 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.