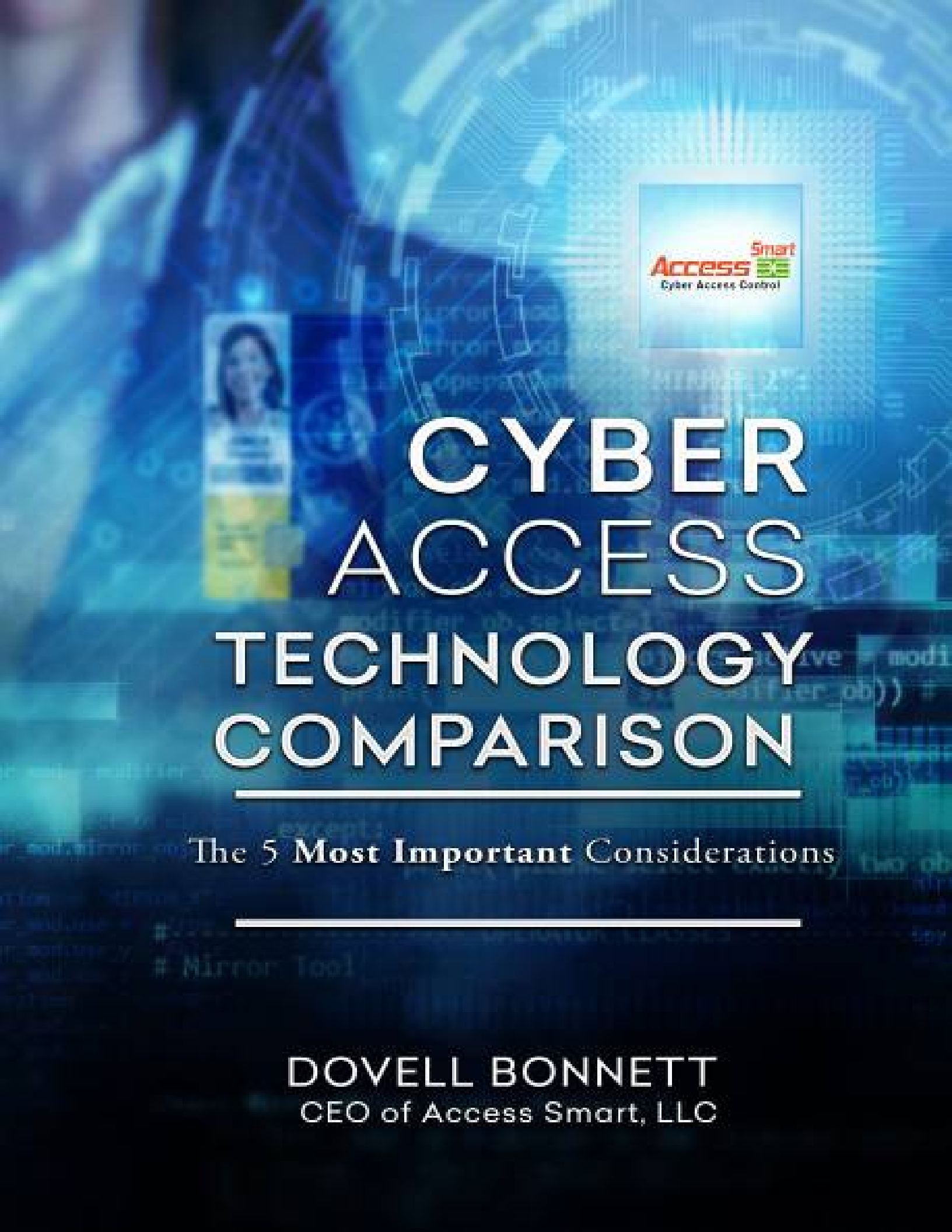


CYBER ACCESS TECHNOLOGY COMPARISON

The 5 **Most Important** Considerations

DOVELL BONNETT
CEO of Access Smart, LLC

The 5 Most Important Considerations

What You Will Learn

This document lays out the essential capabilities of the top four cyber access technologies: Public Key Infrastructure (PKI), One-Time Password (OTP), Single Sign-On (SSO), and Smartcard-based Password Manager (SPM). Before investing in any cyber access solution, you must understand how these different technologies compare in the five most important categories. Those categories are:

1. Purpose and Capabilities
2. Logon Security
3. Backend System Impact
4. End User Systems Considerations
5. Cost of Ownership

Introduction

Cyber Access Control, also known as "Logical Access Control", is the process formally which a computer or network first authenticates that a person or device really is who they claim to be, with a high level of confidence, before access is granted.

IT managers are bombarded daily with numerous government legislations and corporate directives to safeguard computer networks and personal data. Security specialists typically concentrate on back-end security technologies like firewalls, encryption, anti-virus software, spam blockers, secure protocols and more. While all these technologies are important, there is one aspect that is often overlooked: securely authenticating the individual before accessing a computer, network or data. In other words, cybersecurity must begin during computer boot-up. Unfortunately, not all technologies have the ability to securely authenticate *before* the firewall.

The authentication process utilizes three components called "factors":

1. **Something you Have** (Possession based) - a physical item like a card, ID badge or token
2. **Something you Know** (Knowledge based) - a password or PIN
3. **Something you Are** (Inherence based) – biometrics, like a fingerprint, iris or voice print

Using any one of these factors by itself is "Single Factor Authentication" and considered very insecure. Stealing any single factor, no matter which one it is, is relatively easy for a hacker. To increase the hacking difficulty, it is best to combine at least two factors (or all three) before access is granted. The odds of a hacker being in possession of two factors at the same time is remote, and all three is extremely remote. That's why security experts and privacy guidelines all recommend two factors as the *minimum*.

Once the type and number of authentication factors are determined, it's time to understand the four most popular solutions that incorporate Multi-Factor Authentication (MFA) to deliver Cyber Access Control.

The four most common cybersecurity access technologies on the market are:

- **Public Key Infrastructure (PKI)**: uses complex mathematical equations that only another computer can verify. PKI offers Authentication, Authorization, Non-Repudiation, and Data Integrity.
- **One-Time Password (OTP)**: relies on an ever changing password that is valid for seconds or minutes. Short Messaging Service (SMS) where a code is sent to a smartphone is one example of an OTP. OTP offers Authentication and Authorization.
- **Single Sign On (SSO)**: uses the security of networks to store and manage account passwords. SSO offers Authentication, Authorization, and Non-Repudiation.
- **Password Authentication Infrastructure (PAI)**: utilizes the existing password infrastructure, but eliminates the end-user tasks of generating, remembering, typing, and managing passwords. PAI offers Authentication, Authorization, and Non-Repudiation.

Cyber Access Security Considerations

The number one goal of many institutions is to address government security and privacy compliance regulations (e.g. HIPAA, HITECH, FACTA, etc.), and to safeguard against data breaches that could adversely affect a business's reputation (e.g. Sony, Amazon, Bank of America, United States OPM, IRS, DNC, Anthem, Target, etc.).

The second tier of considerations focuses on affordability, limited network modifications and employee ease-of-use. Additional considerations include technical support/ maintenance, employee turnover, and card technologies.

Finally, the third tier of considerations revolve around incorporating other functionalities (like employee ID, physical access and time/attendance) onto a single badge. All the solutions discussed below provide computer network authentication, government privacy compliance and data security. The big differentiators occur where authentication is implemented (before or after boot-up), and around these second and third tier concerns.

Public Key Infrastructure (PKI) is a contact smartcard-based solution that can be incorporated into an employee ID badge and physical access cards. As PKI certificates expire and new ones get issued, files that were secured with old certs cannot be accessed with the new certs, and visa-versa. Therefore, the storage and management of both the old and new certificates must be considered (i.e. the amount of memory available on the chip chosen initially.) Implementing PKI into an existing ID card system requires re-badging or issuing multiple cards because a contact chip must be added to the card.

One Time Passwords (OTP) only works with those servers that are synchronized to the token. Each server requires a separate token. Depending on the complexity of the server network, a single user may have to carry multiple tokens. Because OTP tokens are usually battery powered dongles or thick cards with an LCD display, rarely are they combined with physical access or ID badge systems. With the newer smartphone SMS systems, the user must remember to have the phone charged and accessible to receive the logon code. The mobile industry admits that cloning of a person's smartphone is relatively easy, and it's also easy to infect a smartphone with malware.

Single Sign-On (SSO) is not a card solution but rather software that utilizes active directory or LDAP networks. The advantages are that end-users don't need to remember or enter logon information for *integrated* logon locations. SSO typically uses OTP, PKI or token-based password management (i.e. SMP) for user authentication. The main disadvantages are that SSO cannot be used for initial computer boot-up logons, since a network connection has not yet been established. SSO is limited to only those applications that have been integrated by an IT administrator, it requires constant maintenance to keep it up-to-date with changing user applications, and it must rely on constant network connectivity.

Password Authentication Infrastructure (PAI) offers the flexibility of working with different card technologies like contact smartcards, contactless smartcards, magnetic stripe or 125 kHz proximity technologies. In some cases, rebadging may not be necessary when adding this cyber access solution. The same employee ID badge used for physical access can also be used for cyber access. Plus, there are no certificates to renew or manage and one card will work with multiple servers. With an IT centralized management system, employees don't have to remember, type or know any passwords to any computer, network or server account.

Implementation Considerations

Implementing a cyber access solution requires more than just technology. You have to match the most appropriate technology to the problem you are trying to solve. Here are six additional, non-technical considerations you will also want to address:

1. What are you trying to secure and why?
2. What is the workplace environment?
3. Are there government regulations that have to be met?
4. What is your budget to purchase and maintain a solution?
5. What additional technical training is required?
6. What security infrastructure is currently in place, and how much of it can be leveraged?

The following comprehensive charts address the five most import considerations when deciding which cyber access technology (or technologies) is right for your specific authentication needs. Each of these four cyber access technologies has unique advantages and disadvantages. No single technology is appropriate everywhere or for everyone. And, if the wrong technology is deployed, computer networks and data may actually become *less* secure.

Evaluating these four solutions and understanding the five main considerations will save you time, money, and sleepless nights.

The 5 Most Important Considerations

1. Purpose and Capabilities

Features	Public Key Infrastructure (PKI)	One-Time Password (OTP)	Single Sign-On (SSO)	Password Authentication Infrastructure (PAI)*
Purpose	Increases logon security at point of entry into a network by generating a unique key pair that is tied to a person's personal information called a certificate. Provides support for additional certificate based functions, such as email encryption and digital signatures for documents.	Increases logon security at point of entry into a network by having a server and token generate a unique string of characters that are valid for a short period of time. Does not authenticate the user at boot-up.	Adds ease of use and unified logon security into a network's LDAP (like Active Directory) for one authentication to then access many other logon credentials and passwords. Does not authenticate the user at boot-up.	Authenticates the user at boot-up. Increases logon security for networks, servers, clouds, website and applications. Requires little to no backend server modification.

Features	Public Key Infrastructure (PKI)	One-Time Password (OTP)	Single Sign-On (SSO)	Password Authentication Infrastructure (PAI)*
Capabilities	End-user has a card or token that has cryptographic processing functionality. Card stores a digital certificate and the associated private key, which is 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 to authenticate and unlock the token. The logon process accesses 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, then grants or denies access. Logon during computer boot-up is available, depending on the service used.	End-user has a battery powered token that has a micro-processor and a digital display. Requires a synchronization between the token and a single network server. After pressing a button on the token, display shows a numeric code that the token generates based on a shared secret key and information between server and token. To logon to a network, user must type in the current code number from the token display, plus a PIN. The token authentication server verifies the entered code and PIN, then grants or denies access. Because OTPs require sever connection, authentication can only occur *after* network connection has been established.	Combines ease of use and unified logon security into a network's LDAP (like Active Directory) for one authentication into many other applications, websites, networks, and accounts. Does not authenticate the user when the computer first boots-up.	Removes the employee from having to remember and type logon passwords for computes, applications, web sites, networks, clouds and other accounts. Authenticates the user at boot-up. Which then confirms to the network that a trusted computer and user are connecting. Increases logon security for networks, servers, clouds, website and applications. Requires little to no backend server modification.

2. Logon Security

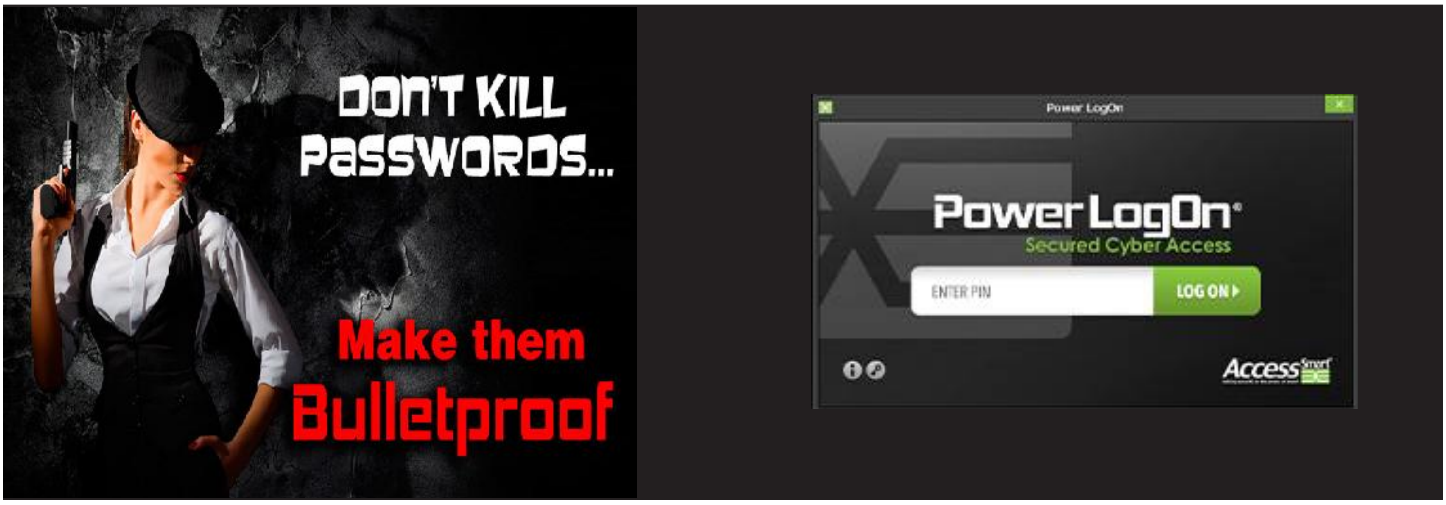
Features	Public Key Infrastructure (PKI)	One-Time Password (OTP)	Single Sign-On (SSO)	Password Authentication Infrastructure (PAI)*
User Authentication Factors	Two-factor, Multi-factor. Token or card, biometrics, and/or PIN.	Double-single factor authentication, not 2FA. User has PIN (knowledge) and code (knowledge). Knowledge + Knowledge equals double single-factor authentication. To get 2FA or MFA, additional hardware and services have to added and integrated together.	Not applicable. Requires separate authentication technology to be used at point of entry.	Two-factor, Multi-factor. Token or card, biometrics, and/or PIN.
Additional Secured Logon Locations	Limited Only secures additional logon locations of systems that have been integrated with, and are secured by, the token authentication server.	Limited Only secures additional logon locations of systems that have been integrated with, and are secured by, the token authentication server.	Limited Only secures additional logon locations of applications that have been integrated with, single sign-on system.	Unlimited End-user stores logon information with card as desired, so additional logon locations can be secured at any time. No administrator integration required.

Features	Public Key Infrastructure (PKI)	One-Time Password (OTP)	Single Sign-On (SSO)	Password Authentication Infrastructure (PAI)*
Logon Security at Point of Entry into Server Network	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 Server 2000 and higher. Process is secured by public/private key pairs, which are generated by and stored on the card chip. The private keys are protected by the card's chip security features. PKI certificates serve as vehicles for the exchange of public keys. Certs 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 the user.	Strong Typically, OTP solutions get the Windows password from the authentication server (or 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 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.	Not applicable.	Strong Logon manager software reads user name, password, and 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 symmetric keys (AES or TDES). Data and keys are additionally protected against unauthorized access by card's internal security features (SSL and SHA Hash). User can specify, securely store, and transfer strong cryptic passwords directly into the logon process.

3. Backend System Impacts

Features	Public Key Infrastructure (PKI)	One-Time Password (OTP)	Single Sign-On (SSO)	Password Authentication Infrastructure (PAI)*
Existing Infrastructure Impact	Very High Must be integrated to work with existing authentication systems and throughout backend system. Requires the purchase of additional server hardware.	Moderately high. Must be integrated to work with existing authentication systems.	Moderate Must be integrated with all linked applications. Need to add in a secure authentication technology like OTP, PKI or SPM.	None Computers, servers, clouds, websites, and applications already have user name and password authentication features enabled. Removes user from role of password manager.
Impact on Physical Access ID Card Infrastructure	High Contact chip has to be embedded into a physical access card. This usually means a total re-badging of all employees. Requires a reader connected to that computer to communicate to cards. PKI enabled chips are more expensive because they require a lot of memory and processing power.	High Requires an expensive specialty token or card to incorporate a display. User carries multiple tokens. One for physical access, and another for cyber access. Two devices for a company to manage. SSO tokens can not work with existing dye sublimation printers for easy on-site issuance. Card uses an internal battery for the display and therefore will have to be replaced.	None SSO is not tied into physical access systems. SSO will require a token for authentication. The impact is dependent on if PKI, OTP or SPM is used.	Low Works with existing contactless or magnetic stripe physical access cards. No impact on the physical access system because re-badging may not be required.

Features	Public Key Infrastructure (PKI)	One-Time Password (OTP)	Single Sign-On (SSO)	Password Authentication Infrastructure (PAI)*
Backend System Components	**Software:** Infrastructure components include a Certificate Authority (CA) for issuing certificates, maintaining certificates, publishing valid certificate owners, maintain revoked and expired certificates. Registration Authority (RA) to verify certificate content. Repository to distribute certificates. Archive to store expired certificates to access historical data. **Hardware:** Hardware Storage Module (HSM) that contains secure co-processors to handle cryptographic algorithms.	**Software:** Random number generator software that is in sync with the displays on the tokens. **Hardware:** Additional secure password generating hardware may be required.	**Software:** 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. **Hardware:** No additional backend server hardware is required.	**Software:** Optional: Card management software can be installed on a server computer for server mode functionality. **Hardware:** No additional backend server hardware is required.



Features	Public Key Infrastructure (PKI)	One-Time Password (OTP)	Single Sign-On (SSO)	Password Authentication Infrastructure (PAI)*
Complexity of Backend System Setup and Maintenance	Very High Company must make a commitment to integrate with backend server system: Public Key network infrastructure must be carefully planned before implementation begins. PKI environment must be configured and certification paths and trust relationships established. Certificates are issued and managed for each user card or token. Any new PKI-aware applications must be integrated as required. PKI must be maintained and adapted to changes in the IT infrastructure. Keys and certificates expire every 1-3 years.	Moderately high. Company must make a commitment to integrate with backend system. 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..	High Company must make a commitment to integrate with backend system. Software must be integrated with existing IT infrastructure. Trust relationships must be established and SSO agents are installed with all application servers. Access rights are configured and maintained for individual users and/or groups. User access rights must be administered and application interfaces configured whenever applications are added or upgraded, or when users and group associations change.	Low Computers, networks, clouds, websites and applications already implement user name and password authentication. No additional integration required. When used with the optional server mode, only a few server settings need to be specified. Only takes IT a few hours to install and learn before they are ready to deploy. Issued licenses do not expire, and with a maintenance contract, licenses are transferable to address employee turnover.

4. End-User System Considerations

Features	Public Key Infrastructure (PKI)	One-Time Password (OTP)	Single Sign-On (SSO)	Password Authentication Infrastructure (PAI)*
End-user System Components	**Software:** Card-specific Crypto Service Provider (CSP) software installed on each end-user computer. **Hardware:** Smartcard or token is issued to each end-user. Contact smartcard or USB token reader installed at each end-user computer.	**Software:** 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. **Hardware:** Token with display required for each end-user. (Note: This must be maintained separately from facility access/ID card and a picture and employee ID# cannot typically be printed on this token.) No computer readers required.	**Software:** Card-specific Crypto Service Provider (CSP) software installed on each end-user computer. **Hardware:** Smartcard or token is issued to each end-user. Contact smartcard or USB token reader installed at each end-user computer.	**Software:** Logon manager software installed on each end-user computer. **Hardware:** Smartcard or token is issued to each end-user. Contact smartcard or USB token reader installed at each end-user computer.
Lifespan and Durability	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.	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.	Not applicable	A contact chip card is vulnerable to physical damage or contamination by liquids. Contactless cards are less vulnerable to environmental conditions. Magnetic stripe cards have a long life and are inexpensive to replace.

Features	Public Key Infrastructure (PKI)	One-Time Password (OTP)	Single Sign-On (SSO)	Password Authentication Infrastructure (PAI)*
Ease of Use	User inserts token or card and enters PIN and/or biometrics for authentication.	Manual entry of code from display is cumbersome and error-prone for end-user. Not 2FA or MFA. At best it is Double-Single Factor Authentication.	Applications that have been integrated with SSO product are immediately accessible, with no need to logon. Users need one of these other authentication technologies.	User inserts card and enters PIN and/or biometrics for authentication. Software auto-records and auto-fills logon information.
Productivity Enhancement	Low Impacts only initial point of entry.	Low Impacts only the initial point of entry.	Moderate Impacts only integrated applications.	High Enhances productivity for all logon locations.

5. Cost of Ownership

Features	Public Key Infrastructure (PKI)	One-Time Password (OTP)	Single Sign-On (SSO)	Password Authentication Infrastructure (PAI)*
Acquisition Costs	Very expensive PKI background administration systems can be costly and complex. Yearly subscriptions. Certificates are non-transferable. Purchase expensive, PKI enabled smartcards. Chips can be integrated with physical access but will require rebadging.	Expensive OTP token systems are proprietary and often costly. Yearly subscriptions. Licenses are non-transferable. Licenses expire. Purchase expensive tokens. Another thing for employee to carry, forget, lose or get stolen.	Moderate to Low Most solutions need agents or connectors for each application. Full acquisition cost consists of license price, plus cost of standard or custom programmed connectors.	Low No added card costs for existing physical access card installations. No subscriptions. Licenses are transferable. Licenses don't expire. Use inexpensive prox, RFID, magstripe or smartcard chips.

Features	Public Key Infrastructure (PKI)	One-Time Password (OTP)	Single Sign-On (SSO)	Password Authentication Infrastructure (PAI)*
Integration and Deployment Costs	Very High Establishing PKI environment must be well planned and can be a lengthy process (CA, trust relationships, Certificate Enrollment Agents, Certificate Revocation Lists, etc.).	Moderate Requires integration with existing authentication system.	Very High Requires establishing interfaces with all integrated applications. Integration of SSO systems with diverse legacy infrastructure can be time consuming and costly.	Low No change to network hardware. No integration of back end system required. Software needs to be loaded.
Operating Costs	Very High Maintenance of complex PKI environment.	Moderate Token expiration and replacements costs, plus maintenance of background authentication system.	Moderate Maintenance of background authentication interfaces.	Low No back-end interfaces to maintain. Re-issue purchased licenses.
Total Cost	Very High	Very High	Moderately High	Low
Who typically uses this approach?	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. Not a viable solution for an SMB.	Larger institutions that are willing to commit to the integration effort with their background system. Institutions that use multiple platforms and legacy systems. Not a viable solution for an SMB.	Larger institutions that have integrated applications, and are willing and able to maintain application links for their end-users. Can be a viable solution depending on the authentication technology used.	Can be used by any size 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.

*In the "Password Authentication Infrastructure" column: when a specific technical approach is cited, it refers to the Power LogOn software product. Note that other password management products may differ in their approach.

Conclusion

Companies that currently use a facility access card or are considering adding one can leverage that investment by adding a Smartcard-based Password Manager for computer and network logon. Stacked up against other Cyber Access Control solutions, the PAI approach compares very favorably.

PAI's multi-factor authentication and strong encryption ensures that logon integrity is maintained and that only the end-user who owns the card will be able to access it. Easy implementation and no back-end server modifications make it convenient and affordable. A wide choice of card technologies offers the flexibility to maintain existing card infrastructures. A card-based password manager is the affordable alternative to PKI and OTP.

Passwords are a secure means of authentication. What has been insecure is how passwords are managed, and who has been allowed to manage them. Companies and agencies can finally remove IT's biggest nightmare – *employee managed passwords*. With PAI, a company can leverage off their existing security infrastructure, avoiding a "Rip 'n' Replace" implementation. Before looking into other authentication technologies that may be cost or time prohibitive, check out Power LogOn by Access Smart as your cybersecurity solution for government compliance, network security and user convenience.

For answers to questions about specific system requirements, contact the author of this report:

Dovell Bonnett
Founder and CEO
Access Smart LLC
www.access-smart.com
Dovell@Access-Smart.com
(949) 218-8754