FEATURE LIST

Sphinx Logon

Windows Logon

Card-secured logon to Windows	End-user presents card to card reader and enters card PIN to logon to websites and applications. Sphinx transfers logon data to logon process transparently so that keystrokes cannot be observed or recorded.
Self enrollment	Sphinx self enrollment screen prompts cardholder to present existing card to card reader, type in Windows user name and password, and specify PIN. Then after next system reboot, Sphinx prompts cardholder to present card and enter PIN to logon to Windows. No need for administrator to collect or re-issue ID badges.
Pull card to lock, logoff, or shutdown computer	End-user can remove card from reader to lock, logoff, or shutdown workstation. Setting can be established by Administrator in Sphinx administrator software or by end-user in Sphinx Logon software, as required. Administrator can specify if end-user will be allowed to change this setting.
Pull card to lock, logoff, disconnect from Terminal Services session	End-user can remove card from reader to lock, logoff, disconnect, or shutdown from a Terminal Services session. Administrator can specify if end-user will be allowed to change this setting. Administrator also has the option to specify that a custom script will be launched upon card removal, also triggering a disconnect of the remote session if desired.
Lock, logoff, shutdown, disconnect with presence detection devices	In addition to card-removal behavior, workstation can also be locked using an optional sonar device or kiosk mat that detects when end-user steps away from workstation. Sphinx works seamlessly with these devices.
Tap in / tap out	Tap card on reader to logon. Tapping reader with card again, when this option is activated, triggers the "pull card" action that was specified (as described above).
Control Windows "secure screen saver" and "lock workstation" functions from Sphinx	End-user can "lock" Windows session before stepping away from their desk using Sphinx short-cut button. End-user can "unlock" a Windows session that has been locked by Windows "secure screen saver" or “lock computer" functions by presenting card and entering card PIN.
Password change reminder	Sphinx can prompt cardholder to change Windows password every specified number of days. Setting can be established by end-user in Sphinx Logon software or by Administrator in Sphinx administrator software, as required. Administrator can specify if end-user will be allowed to change this setting.
Generate random Windows password	When end-user or Administrator changes Windows password, they can generate a random password that conforms to the installation's Windows password policy, if applicable. If installation has no Windows password policy, they can specify password length and character type (numeric, upper case, lower case...) for random password.
Windows password change synchronization	When a Windows password is changed in the Sphinx Logon or Sphinx administrator program, password change will be synchronized with Windows. Likewise, if Windows

	informs end-user at start-up that their password has expired and end-user changes password as prompted, password change will be synchronized with Sphinx.
Stores multiple Windows logons	For end-users with multiple Windows logon identities or domains, Sphinx allows entry and selection of multiple logons.

Windows Logon Management

Easy management	The Windows logon user name and password cardholder enters during self enrollment will automatically create a managed entry in Sphinx. Administrator can then choose to take over management and updating of Windows passwords, or can allow end-user to manage Windows password.
Non-intrusive protection	Does not replace or change Microsoft authentication process, only interacts with relevant functions. No change to network or infrastructure required.
Windows password policy control	Administrator can specify required Windows password length and character type (numeric, upper case, lower case...) in Sphinx administrator software, and end-user must conform to these requirements when entering or changing Windows password.
Password repetition control	Sphinx can prohibit the entry of up to four previously used Windows passwords, when cardholder changes Windows password. Administrator can establish setting in Sphinx administrator software.
Cardholder logon / logoff report	Sphinx logs when end-users logon to Windows and logoff of Windows with their card. This record can be viewed as an administrator transaction report.
Create new random Windows password upon first use and at defined intervals	Administrator can specify that upon first use of an end-user card, a new random Windows password that conforms to the installation's Windows Password Policy, if applicable, will be generated for that end-user. Administrator can also define that a new random Windows password will be automatically generated for the end-user after a defined interval of time. This is a popular feature amongst security-minded administrators since, with this scenario, end-users no longer know their Windows password and can subsequently only logon to the network with their card.
Sychronized Active Directory enrollment for Windows logon	When this option is activated, when administrator issues a card from the administrator software, the system automatically creates a new Windows user account in Active Directory. Ie, once the end-users have the cards in their hands, all cards can immediately be used to logon to network computers. This feature is especially suitable for campuses for example, where photo ID cards are issued to a large number of incoming end-users at once. Administrator can specify if end-user will be allowed to view or change the logon data.
Logon Entries Wizard	Administrator can pre-enter logon entries for additional Windows logons for individuals or a user group, and the Sphinx Logon Entries Wizard will prompt the cardholders to personalize the entry with their user name and/or password when they open the Sphinx Logon software. Wizard entries can be loaded to card accounts at any time.

Website and Application Logon

Card-secured logon to websites and applications	End-user presents card to card reader and enters card PIN to logon to websites and applications. Sphinx transfers logon data to logon process transparently so that keystrokes cannot be observed or recorded.
End-user managed logon entries	By default, cardholder is prompted to auto-record their logon data for websites and save it to their Sphinx account. Application logon data is easily recorded using the Record button. The next time cardholder goes to a website or application that Sphinx knows, cardholder is prompted to present card and enter PIN to logon to website or application. Note: Logon data which end-user saves with Sphinx cannot be accessed by Administrator.
Auto-record and auto-fill of logon data	Whenever cardholder enters logon information into a website that Sphinx recognizes as being recordable, Sphinx asks cardholder if he wants to record the logon data. Whenever cardholder goes to a website or application logon location which Sphinx has recorded, Sphinx prompts cardholder to present card and enter PIN, then automatically enters logon data and cardholder is logged on.
Initiate recording of logon data	It's easy to record application logon data using the Record button. Or, end-users who don't want to use the auto-record feature for website logons can switch off this default setting, and click on the Record button to initiate the recording of logon data. The Record button is also useful for websites that don't adhere to typical logon procedures, that Sphinx doesn't recognize as being recordable. In any case, whenever cardholder goes to a logon location which Sphinx has recorded, Sphinx prompts cardholder to present card and enter PIN, then automatically enters logon data and cardholder is logged on.
Manual entry and button-click fill of logon data	For website or application logon locations that don't have a unique address, it's simple for cardholders to create a new logon entry in Sphinx and manually enter logon data. Then to fill logon data, simply open the logon entry in Sphinx and click on the Sphinx "Logon Now" button to transfer logon data to location.
Browse to logon location from Sphinx	End-user can double-click on a website or application entry in Sphinx to browse to that location or start application, and auto-fill or transfer logon data.
Sphinx pop-up	Whenever cardholder goes to a website or application logon location that Sphinx has stored but which is not designated as auto-fill, Sphinx automatically pops-up with the logon data so that cardholder can complete logon.
Submit control	Cardholder can choose to submit logon data to logon processes automatically, or can choose to manually control the submission of logon data. With the latter option, cardholder must click on the website or application "Submit" or "Enter" button, to submit logon data. Manually controlled submission of logon data is the default for auto-filled entries.
"Drag and drop" transferal of logon data	Logon data fields can be "dragged and dropped" into logon entry fields as desired.
Generate random password	When end-user or Administrator creates or changes a website or application password, they can generate a random password which conforms to the installation's Password Policy, if applicable. If installation has no Password Policy, they can specify password length and character type (numeric, upper case, lower case...) for random password.

Password change reminder	Sphinx can prompt cardholder to change website or application password every specified number of days. Setting can be established by end-user in Sphinx Logon software or Administrator in Sphinx administrator software, as required. Administrator can specify if end-user will be allowed to change this setting.
Password change verification	Sphinx can prompt cardholder to verify that password has been changed in website or application. This ensures that passwords remain synchronized (since it would not be possible for Sphinx to automatically change a password in a third party website/application logon location that is not linked to Sphinx via an API). Until cardholder verifies that password has been changed in website/application, Sphinx will not accept password change. Setting can be established by end-user in Sphinx Logon software or Administrator in Sphinx administrator software, as required. Administrator can specify if end-user will be allowed to change this setting.

Website and Application Logon Management

Administrator managed logon entries	Administrator may choose to preset logon entry data and load it to end-user Sphinx accounts. Administrator can also continue to manage logon data for cardholders if desired, by updating logon data in cardholder account. For entries created by Administrator, Administrator can specify if end-user will be allowed to view or change the logon data. See also Managed Entry Features.
Logon Entries Wizard	Administrator can pre-enter logon entries for individuals or a user group, and the Sphinx Logon Entries Wizard will prompt the cardholders to personalize the entry with their user name and/or password when they open the Sphinx Logon software. Wizard entries can be loaded to card accounts at any time.
Password policy control	Administrator can specify required password length and character type (numeric, upper case, lower case...) for websites/applications in Sphinx administrator software, and end-user must conform to these requirements when entering or changing passwords.
Password repetition control	Sphinx can prohibit the entry of up to four previously used passwords, when cardholder changes a website or application password. Administrator can establish setting in Sphinx administrator software.

Other End-user Features

No training required	End-user interface is intuitive and easy to use. Software prompts guide end-user through program.
Auto-start and minimize	Sphinx Logon automatically starts at system startup, so that it is available for logons throughout the session. After auto-start, software automatically minimizes to the system tray. Thereafter, Sphinx auto-fills logon data or end-user double-clicks on Sphinx icon to access software, as required. These default setting can also be switched off according to user preference. Administrator can control auto-start capability as desired in the Sphinx administrator software.
Storage of address and	End-user stores address and payment information in Sphinx, for use in website and

payment information	application entry fields. The labels of all address and payment entry fields can be customized by the end-user. Cardholder can "drag" address and payment information and "drop" it into website and application entry fields, so that this basic information does not have to be continually re-typed.
Backup and restore data	Cardholder can back up all of his Sphinx data to his computer's hard drive, the network, or a removable data carrier such as a memory stick. Sphinx prompts cardholder to enter a backup password. Then, if he forgets the authentication data for his contactless card or loses his contact chip card or, he can restore his Sphinx data to a new card as long as he knows his backup password. Setting of backup location can be established by end-user in Sphinx Logon software or Administrator in Sphinx administrator software, as required. Administrator can specify if end-user will be allowed to change this setting.
Auto-backup reminder	Sphinx can prompt cardholder to backup his Sphinx data every specified number of days at a certain time of day, or after data has been saved to Sphinx a specified number of times. Setting can be established by end-user in Sphinx Logon software or Administrator in Sphinx administrator software, as required. Administrator can specify if end-user will be allowed to change this setting.
Save Sphinx data to laptop	For card installations that use the Sphinx administrator server to store Sphinx entries, cardholders have the option to save their Sphinx data to Laptop Mode, so that they can use Sphinx to access this data while they travel with their laptop. Administrator also has the option to disable Laptop Mode, or require that a card and card reader is also required in Laptop Mode, and can specify this setting in the Sphinx administrator software.
Access Sphinx server remotely over internet	At installations that have a public IP, or use VPN or Remote Desktop, end-users can logon with their card and card reader from a remote location.
Access Sphinx server with remote access mode	The remote access mode feature enables user to access Sphinx data on server without a card or card reader, when traveling. For security reasons, this option is typically only made available upon user request - for example, if user forgot to load Sphinx data to laptop before leaving headquarters. Administrator can activate this capability on an individual basis for a defined period of time in the Sphinx administrator software.
One time password	The remote access mode can be configured to send a One Time Password to the user via email or text message (SMS). The RA-OTP configuration ensures that the user's Sphinx data is still protected via a two-factor authentication mechanism even when a card/reader is not available. Administrator can activate this capability on an individual basis for a defined period of time in the Sphinx administrator software.

Setup Features

Easy installation of end-user software	Pre-configured Sphinx Logon software self-installs at end-user computers and is ready for immediate use, with no additional configuration required. Because the Sphinx Logon setup is based on Microsoft Installer, it can easily be rolled out to all

	end-user computers on a network.
Easy installation of administrator software	Pre-configured Sphinx administrator software self-installs at administrator server computer. Administrator specifies only three server settings, imports license keys, and software is ready for immediate use, with no additional configuration required. Administrator can further choose from a wide pallette of feature options as desired.
Administrator program protection	Administrators logon to Sphinx administrator using Administrator password, or based on the administrator rights granted to their card. Primary Administrator grants or revokes Sphinx administrator rights for other Administrators. Activity log automatically records which administrator performed each activity.
Standalone option	Installations that do not have networked computers can also use the Sphinx software to logon to Windows, websites, and applications. In Standalone mode, Sphinx data is encrypted and saved to the local computer. Users self enroll by entering their Sphinx license key. Sphinx server functionality, such as managed entries, would not be available.

Enrollment

Self-enrollment options	By default upon first use, cardholder presents card to card reader and is prompted to enter Windows user name and password to register with Sphinx server. Administrator can change the default settings, to also require entry of name and employee ID#, as desired. This information (except for Windows password) will populate the Sphinx cardholder database. Sphinx software is then ready for immediate use.
User group control	Administrator can specify different default card settings and managed entries for different user groups, for example, "Sales Department" or "Management".
Lost or stolen card "hotlist"	When a card is lost or stolen, it can be reported to the Sphinx administrator software so that it will no longer be accepted within the Sphinx system.
Self re-enrollment with new card	After a card has been reported as lost or stolen, end-user can self re-enroll with Sphinx and access his previous Sphinx data if he knows his PIN. Note: Standalone users must have a backup of their previous Sphinx data and know their backup code, if they want to use previous data with their new card.
Card recycling	All Sphinx card data can be erased using the Sphinx administrator software, so that the card can be re-used and issued to another user.
License re-use	Whenever a card is recycled using the Sphinx "recycle" function, the Sphinx license from that card is also returned to the available license count. So even if you don't want to re-use a card, you can still re-use the Sphinx license. Note that cards must be present in order to reclaim Sphinx licenses using the "recycle" function.
Card issuance from admin station	Administrators can also opt to assign and re-issue cards to end-users using the "Issue Card" function in the Sphinx administrator software.
ID card printing	Administrator has the option to print ID cards as a part of the issuance step, using a TWAIN compatible webcam and an ID card printer. Allows for full color printing on one side, with photo, name, ID#, and additional fields as desired.
Reports	Complete cardholder reports and transaction logs are available in the Sphinx

	administrator software.

Managed Entries

Easy creation of managed entries	Administrator simply creates a logon entry using the Sphinx Logon software and saves it. When the adminstrator "auto-records" the logon entry, Sphinx "learns" the logon location of the entry, and the formats for user name, password and other entry fields.
Easy assignment of managed entries to user groups or individuals	Administrator assigns managed entries to user groups or individuals, and edits user name and password information as required for the group or individual. Administrator can specify if user group or individual will be allowed to view, edit, or delete the managed entry.
Simple managed entry screen	Managed entries are easy to edit using the Managed Entries screen in the Sphinx administrator software, where Administrator has an overview of all managed entries and can easily select, edit, and assign managed entries.
No additional programming required	Many other logon management systems require that the administrator program links to the applications for which logon entries will be managed. No programming is required with Sphinx. The managed entries functionality works as easily as all of the other Sphinx features.
API for automatic provisioning	All managed entries are available via an API for 3rd party identity management and provisioning systems, which can enable automatic provisioning of logon data to applications. Interfaces are based on ODBC, LDAP and XMP-RPC standards.

Wide Compatibility

RFID cards	Works with most RFID contactless cards out-of-the-box. RFID cards are by far the most popular choice of customers since this allows them to use one card for both building access and network authentication. Does not impact existing RFID card setup. Sphinx data is stored on the administrator server for RFID cards, so end-users can access their Sphinx data from any workstation on a network.
Smart cards	Contact chip smart cards or tokens can be used in two modes: storing data on the card, or using the smart card simply to authenticate to the Sphinx server. Storing data on a smart card has the portability advantage, since that data can be used at any workstation anywhere the Sphinx software is installed. Smart card readers may also be less expensive. The main disadvantage is that none of the Sphinx server functionality is available and Administrators cannot easily manage logon entries for smart cards. The Logon Entries Wizard can however be used to load entries upon card issuance, and the Load Logon Entries feature may be used to load further entries. Using a smart card to simply authenticate to the Sphinx server enables the Administrator to fully manage logon entries for end-users. Installations that don't have ID cards can opt for a compact USB token device, for example, bypassing the need for both a card and reader.
PKI cards and middleware	Works out-of-the-box with most PKI cards and can be used side by side with PKI functionality. For example, if you logon to Windows with a PKI certificate, you can

	then use Sphinx to logon to websites and applications.
Card readers	Works with most PC/SC compatible card readers out-of-the-box. A wide variety of form factors can also be considered, for example tiny readers for laptops, RFID tags and USB sticks.
Biometric	A biometric device such as a fingerprint or iris reader can be used for end-user authentication, either in combination with a card and/or PIN or by itself. Full biometric capabilities are completely integrated into the Sphinx software and work out-of-the-box with selected BIO-API compatible devices, including biometric enrollment and authentication.
Other devices	Presence detection devices, such as a sonar camera or a kiosk mat, can be used to trigger the closing of an end-user session when end-user steps away from the workstation.

Security Features

User designated PIN	By default upon first use, cardholder is prompted to choose a unique Personal Identification Number (PIN). This PIN, along with presentation of the card, will be required for all access to the Sphinx Logon software. A card will be locked and no longer accepted within the Sphinx system if the cardholder enters the wrong PIN multiple times.
PIN policy control	Administrator can specify required PIN length and character type (numeric, upper case, lower case...) in Sphinx administrator software, and end-user must conform to these requirements.
PIN verification timeout	Specifies the length of time that a PIN will be stored in memory. After this time, end-user will be prompted to re-enter PIN. Setting can be established by end-user in Sphinx Logon software or Administrator in Sphinx administrator software, as required. Administrator can specify if end-user will be allowed to change this setting.
Easy PIN reset	If an end-user forgets his PIN, administrator can reset PIN from administrator software.
PUK option	The PUK is a second card PIN, which the cardholder can use to unlock their card. Once a card has been locked, Sphinx will prompt the cardholder to enter the PUK to unlock the card. By default, Sphinx generates a random PUK for each cardholder and stores it in the administrator software. Administrators can pass this PUK along to end-users as desired, for example, for use if Administrator is occasionally not available to reset a PIN.
Randomly generated PIN/PUK option	Most Sphinx installations use the standard default initial PIN of "12345", which the end-user is prompted to change upon first use. This is typically appropriate for self enrollment, or when a card that was issued from the administrator software does not yet contain any personalized data. Installations which want to specify a different initial PIN/PUK for each card that is issued from the administrator software - for example, installations that pre-load information to the card or card account - have the option to generate a random PIN/PUK for each card. A PIN letter is automatically generated in the Sphinx administrator software that can then be emailed or delivered to the end-user.

	Cardholders with randomly generated PIN/PUKs will not be prompted to change their PIN and PUK upon first use, but this is recommended, since the initial PIN and PUK will be the same. Not available for cards that self enroll.
Secure handling	Each issued Sphinx card or Sphinx account is secured by its own unique set of encryption keys. Communication between the Sphinx Logon client and the Sphinx administrator server is secured by encryption methods and key handling protocols that adhere to the Federal Information Processing Standard (FIPS) 140-2 U.S. issued by the National Institute of Standards and Technology (NIST). The applied cryptographic security is based on government strength AES 256 encryption and SHA 256 hashing algorithms. Only FIPS 140-2 validated cryptographic modules are used to protect the credential data in transit and at rest. The Sphinx client / server security protocol includes mutual cryptographic authentication based on random-number challenge / response handshakes, key diversification, and use of temporary session keys.
Connection to secure server protected by SSL	Installations can choose to additionally secure the data exchange between client and server via SSL.

Other Software Features

Database importing	Employee data can be imported from HR database into Sphinx administrator software before card issuance, if required. Built-in data import functions support ODBC and LDAP compatible databases. Sphinx administrator can also be linked with facility access control card management system if desired.
SQL Server ready	Sphinx administrator can optionally utilize a customer's own SQL Server database instance or a dedicated SQL Server Express.
Customized logo option	Upon request Sphinx can be delivered with a customized logo provided by customer.
Multi-language	Sphinx multi-language tool enables convenient translation and maintenance of the Sphinx program text files, including Asian languages with double-byte characters. Also enables easy branding of software for OEMs.
Sphinx Logon API for OEMs	OEMs who want to bundle Sphinx with other client applications have the option to use the built-in API to integrate further.
Sphinx administrator API for third-party applications	Data elements of the Sphinx administrator database are accessible through standard ODBC API. Sphinx administrator features a flexible, built-in import function for LDAP and ODBC based data soruces. This means that, for example, cardholder identification data can be imported from an HR or access control database without requiring any programming. All managed entries are available via an API for third party identity management and provisioning systems. Interfaces are based on ODBC, LDAP and XMP-RPC standards.

052021