SPHINX Feature List

Sphinx Versions

The Sphinx software is available in three versions, to meet the needs of all types and sizes of organizations.
The list below indicates the features that are included in each Sphinx version. See also www.odsphinx.com for additional information.

Version	Order #	Description	Included software components
Sphinx Standalone	S-20	No management or issuance system required. • Install Sphinx Logon Manager software and desktop card readers on end-user computers. • End-users present their IDs card to card readers to self-enroll with Sphinx, and start protecting their logon data.	Sphinx Logon Manager, for end-user computers
Sphinx Enterprise	S-30	Easy setup and self-enrollment features of Sphinx Standalone version, plus: • Pre-configured Sphinx CardMaker management software, runs "out-of-the-box" on administrator server computer. • Administrators who want more control can change the default settings of this full-featured software to specify PIN and password policies, link to HR databases, and much more.	Sphinx Logon Manager, for end-user computers Sphinx CardMaker, for administrator computer
Sphinx Enterprise PKI	S-30-PKI	All functionality of Sphinx Enterprise version plus: • PKI card interface and "middleware" is built-in, enabling the ID card to support the full spectrum of certificate-based functions, such as email encryption and digital signatures for documents.	Sphinx Logon Manager, for end-user computers Sphinx CardMaker, for administrator computer PKI middleware, for all computers

Windows Logon Features

Feature	Description	Sphinx Standalone	Sphinx Enterprise	Enterprise PKI
GINA-based logon to Windows	End-user presents card to card reader and enters card PIN to logon to Windows. Sphinx transfers logon data to Windows logon process transparently so that keystrokes cannot be observed or recorded. Standard Sphinx installations use Microsoft GINA-based logon to Windows. Sphinx 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.	✓	✓	✓
Certificate-based logon to Windows	When Sphinx is used with a Public Key Infrastructure (PKI), the Sphinx PKI middleware provides standard CSP and PKCS#11 card interfaces, which enables the card to be used for certificate-based functions. End-user presents card to card reader and enters card PIN to logon to Windows. 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. See also PKI Features.			✓
End-user managed Windows logon data	Upon first use, cardholder uses Sphinx QuickStart guide to easily enter their existing Windows logon data into Sphinx program. With next system reboot, cardholder is prompted to present card and enter PIN to logon to Windows. Note: logon	✓	✓	✓

	data which end-user saves with Sphinx cannot be accessed by Administrator.			
Administrator managed Windows logon data	Available with Sphinx CardMaker software version 3.1 (release 10/05). Administrator may choose to preset Windows logon entry data for individuals or groups of cards. Administrator can also continue to manage Windows logon data for cardholders if desired, by updating Windows 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.		✓	✓
Storage of multiple Windows logons	For end-users with multiple Windows logon identities or domains, Sphinx allows entry and selection of multiple logons.	✓	✓	✓
Pull card to lock, logoff, or shutdown computer	End-user can remove card from reader to lock, logoff, or shutdown workstation. Removal of card invokes the appropriate Windows process. Setting can be established by end-user in Sphinx Logon Manager software or by Administrator in Sphinx CardMaker software, as required. Administrator can specify if end-user will be allowed to change this setting. In addition to card-removal behavior, workstation can also be locked using an optional sonar device that detects when end-user steps away from workstation. Sphinx is also compatible with this device.	✓	✓	✓
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.	✓	✓	✓
Windows password change synchronization	When end-user changes Windows password in the Sphinx program, password change will be synchronized with Windows so that end-user does not need to enter the change twice. Likewise, if Windows prompts end-user to change Windows password, and Sphinx program is currently active, password change will be synchronized with Sphinx program.	✓	✓	✓
Windows password policy control	Administrator can specify required Windows password length and character type (numeric, upper case, lower case...) in Sphinx CardMaker software, and end-user must conform to these requirements when entering or changing Windows password.		✓	✓
Generate random Windows password	When end-user changes Windows password, he can generate a random password that conforms to the installation's Windows Password Policy, if applicable. If installation has no Windows Password Policy, end-user can specify password length and character type (numeric, upper case, lower case...) for random password.	✓	✓	✓
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 Manager software or by Administrator in Sphinx CardMaker software, as required. Administrator can specify if end-user will be allowed to change this setting.	✓	✓	✓
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 CardMaker		✓	✓

	software.			

Website and Application Logon Features

Feature	Description	Sphinx Standalone	Sphinx Enterprise	Enterprise PKI
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	Cardholder uses Sphinx QuickStart guide to easily auto-record their logon data for websites and applications and save it to their Sphinx account. 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.	✓	✓	✓
Administrator managed logon entries	Available with Sphinx CardMaker software version 3.1 (release 10/05). 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.		✓	✓
Auto-record and auto-fill of logon data	Whenever cardholder enters logon information into a website or application that Sphinx recognizes as being recordable, Sphinx asks cardholder if he wants to record the logon data. Then, whenever cardholder goes to a website or application logon location which Sphinx has stored, Sphinx automatically enters logon data and cardholder is logged on.	✓	✓	✓
Initiate recording of logon data	End-users who don't want to use the auto-record feature can switch off this default setting, and click on the Sphinx "Record" button to initiate the recording of logon data.	✓	✓	✓
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 manually enter logon data into Sphinx, and then click on the Sphinx "Logon Now" button to transfer logon data to location.	✓	✓	✓
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.	✓	✓	✓
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.	✓	✓	✓
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.	✓	✓	✓

Password policy control	Administrator can specify required password length and character type (numeric, upper case, lower case...) for websites/applications in Sphinx CardMaker software, and end-user must conform to these requirements when entering or changing passwords.		✓	✓
Generate random password	When end-user changes website or application password, he can generate a random password which conforms to the installation's Password Policy, if applicable. If installation has no Password Policy, end-user 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 Manager software or Administrator in Sphinx CardMaker 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 Manager software or Administrator in Sphinx CardMaker software, as required. Administrator can specify if end-user will be allowed to change this setting.	✓	✓	✓
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 CardMaker software.		✓	✓

Other End-user Features

Feature	Description	Sphinx Standalone	Sphinx Enterprise	Enterprise PKI
Storage of address and payment information	End-user stores address and payment information in Sphinx, for use in website and application entry fields. The labels of all address and payment entry fields can be customized by the end-user.	✓	✓	✓
"Drag and drop" transferal of address and payment information	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 or floppy disk. Sphinx prompts cardholder to enter a backup password. Then, if he loses his contact chip card or forgets the authentication data for his contactless card, 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 Manager software or Administrator in Sphinx CardMaker 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 Manager software or Administrator in Sphinx CardMaker 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 CardMaker 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 without a card, card reader or network connection 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 CardMaker software.		✓	✓
Access Sphinx data on CardMaker server remotely	For card installations that use the Sphinx CardMaker server to store Sphinx data, this 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 CardMaker software.		✓	✓
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 Manager software 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.	✓	✓	✓

PKI Features

Feature	Description	Sphinx Standalone	Sphinx Enterprise	Enterprise PKI
One step installation of middleware software	PKI middleware software self-installs at end-user and administrator computers and is ready for immediate use, with no additional configuration required.			✓
Seamlessly integrated with Sphinx	The Sphinx PKI middleware has been fully integrated with the Sphinx software in the Sphinx Enterprise PKI version. End-users can use Sphinx Logon Manager software functionality and PKI functionality seamlessly together using a single card. Administrators manage the solution using the Sphinx CardMaker software interface. Note: Features described under Windows Logon Features refer to GINA-based logon features. Certificate-based Windows logon features that an organization chooses to implement will be independent of the GINA-based logon features.			✓
Standards based	Includes PKCS#11 library, and Cryptographic Service Provider (CSP) for applications supporting Microsoft CryptoAPI. Supports all major standards and interfaces including PKCS			✓

	#11, Microsoft CryptoAPI, PC/SC, PKCS #12, PKCS #15.			
Secure storage	On-board cryptographic key generation up to 2,048 bit. Secure storage of X.509 digital certificates. Multiple key and certificate storage.			✓
Seamless Windows compatibility	Fully transparent Windows logon (2000, XP, 2003). Seamless integration in Windows: secure user authentication, e-mail signing and encryption, VPN, network access, logon, and Terminal Services (Windows 2003).			✓
Supported PKI systems	Baltimore, Entrust, eTrust, Global Sign, Microsoft, RSA, SafeGuard, SafeLayer, Verisign.			✓
Supported applications	VPN: Check Point, Cisco, Microsoft, NCP. Secure e-mail clients: Microsoft Outlook (98, 2000, XP, Express), Novell Groupwise 6, Baltimore MailSecure, Netscape Messenger, Mozilla Mail. SSL authentication for browsers: Microsoft Internet Explorer, Netscape Navigator, Mozilla Navigator, Mozilla Firefox. Other applications: Citrix, Lotus Notes, PGP, SSH Tectia Client, RSA SecurID.			✓
Interoperability	Works out-of-the-box with a diversity of state-of-the-art cards and tokens. See Solution Packages at www.odsphinx.com.			✓

Setup Features

Feature	Description	Sphinx Standalone	Sphinx Enterprise	Enterprise PKI
Easy installation of end-user software	Pre-configured Sphinx Logon Manager software self-installs at end-user computers and is ready for immediate use, with no additional configuration required. Sphinx Logon Manager setup is based on Microsoft Installer, which is compatible with numerous network installation tools.	✓	✓	✓
Easy installation of administrator software	Pre-configured Sphinx CardMaker software self-installs at administrator server computer. Administrator specifies only three server settings and software is ready for immediate use, with no additional configuration required.		✓	✓
No change to network or Windows setup	Requires no change to existing network setup or user accounts on domain server. Requires no change to existing Windows setup. Logon to Windows performs according to standard Windows protocols for Standalone as well as networked computers (NT Domain Servers, Active Directory).	✓	✓	✓
No change to RFID card setup	Requires no change to existing configuration of RFID cards that are compatible with Sphinx. Cardholders can self-enroll with Sphinx using the cards they already have, with no administrator involvement. The added logical access functionality with Sphinx does not impact on any other RFID card functions (such as facility access control, time & attendance or e-purse functions). When a Sphinx installation is setup to store data on the card, Sphinx can be pre-configured to only use the available free sectors on the card.	✓	✓	✓

Auto-enrollment Features

Feature	Description	Sphinx Standalone	Sphinx Enterprise	Enterprise PKI
No configuration required	Software is pre-configured with standard default settings and ready for end-user self-enrollment immediately after installation.	✓	✓	✓
End-user self-enrollment	Upon first use, cardholder presents card to card reader and is prompted to enter name and employee ID# to register with Sphinx. Cardholders with Sphinx Standalone version will also be prompted to enter their Sphinx license key. Sphinx software is then ready for immediate use.	✓	✓	✓
End-user self re-enrollment	If end-user loses his card and is given a new card, he can self re-enroll with Sphinx and access his previous Sphinx data if he knows his personal security code. 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.	✓	✓	✓

Managed Enrollment Features

Feature	Description	Sphinx Standalone	Sphinx Enterprise	Enterprise PKI
Customizable settings	Installation can use manufacturer's software default settings. Or, Administrator can change software settings in Sphinx CardMaker software before issuing cards, to reflect corporate security policies and control how the end-user uses Sphinx.		✓	✓
Database importing	Employee data can be imported from HR database into Sphinx CardMaker software before card issuance, if required. Built-in data import functions support ODBC and LDAP compatible databases. Sphinx CardMaker can also be linked with facility access control card management system if desired.		✓	✓
User groups	Administrator can specify different default card settings and managed entries for different user groups, for example, "Sales Department" or "Management".		✓	✓
One step issuance	Administrator clicks "Issue Card" in Sphinx CardMaker software and chooses end-user from database, or enters end-user data, to issue card.		✓	✓
Lost or stolen card "hotlist"	When a card is lost or stolen, it can be reported to the Sphinx CardMaker software so that it will no longer be accepted within the Sphinx system.		✓	✓
One step card re-issuance	After a card has been hotlisted, a new card can be re-issued to the cardholder by selecting the cardholder's name from the cardholder list.		✓	✓
Recycle card	All Sphinx card data can be erased using the Sphinx CardMaker software, so that the card can be re-used and issued to another user.		✓	✓
Reports	Complete cardholder reports and transaction logs are available in the Sphinx CardMaker software.		✓	✓

Managed Entries Features

Available with Sphinx CardMaker software version 3.1 (release 10/05).

Feature	Description	Sphinx Standalone	Sphinx Enterprise	Enterprise PKI
Easy creation of managed entries	Administrator simply creates a logon entry using the Sphinx Logon Manager 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.		✓	✓
Simple managed entry screen	Managed entries are easy to edit using the Managed Entries screen in the Sphinx CardMaker software, where Administrator has an overview of all managed entries and can easily select, edit, and assign managed entries.		✓	✓
End-user edit control	Administrator can specify if user group or individual end-user will be allowed to view, edit all, edit password, or delete the managed entry.		✓	✓
Storage control	Administrator can specify if the managed entry will be stored on the end-user card and on the server, or stored only on the Sphinx server.		✓	✓
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 identity management systems	All managed entries are available via an API for 3rd party identity management and provisioning systems. Interfaces are based on ODBC, LDAP and XMP-RPC standards.		✓	✓

Other Administrator Features

Feature	Description	Sphinx Standalone	Sphinx Enterprise	Enterprise PKI
Administrator program protection	Administrators logon to Sphinx CardMaker using Administrator password, or based on the administrator rights granted to their card.		✓	✓
Administrator assignment	Primary Administrator grants or revokes Sphinx CardMaker rights for other Administrators.		✓	✓
Activity log	When Administrators logon to Sphinx CardMaker with their card, the activity log automatically records which administrator performed each activity.		✓	✓

Security Features

Feature	Description	Sphinx Standalone	Sphinx Enterprise	Enterprise PKI
User designated PIN	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 Manager software.			
User designated PUK	Upon first use, cardholder is prompted to choose a unique Personal Unlock Key (PUK). The PUK is a second card PIN, which the cardholder can use to unlock their card. A card will be locked and no longer accepted within the Sphinx system if the cardholder enters the wrong PIN multiple times. Once a card has been locked, Sphinx will prompt the cardholder to enter the PUK to unlock the card.	✓	✓	✓
Randomly generated PIN option	Most Sphinx installations use a standard default initial PIN of "12345", which the end-user is prompted to change upon first use. This is typically appropriate when the card that was issued does not yet contain any personalized data. Installations which want to specify a different initial PIN for each card that is issued - for example, installations that pre-load information to the card or card account - have the option to generate a random PIN for each card. A PIN letter can be generated in the Sphinx CardMaker software that can then be delivered to the end-user. Cardholders with randomly generated PINs will also be prompted to change their PIN upon first use. In both of the above cases, the initial PIN and the PUK will be the same, but the cardholder will be prompted to change each individually.		✓	✓
Require PIN/PUK change upon first use option	All Sphinx installations prompt end-user to change the initial PIN and PUK upon first use. Installations that require an additional level of control can select the Sphinx CardMaker option which will require that the end-user change the PIN/PUK upon first use. In this case, if the PIN/PUK is not changed, the program will not continue.		✓	✓
PIN policy control	Administrator can specify required PIN length and character type (numeric, upper case, lower case...) in Sphinx CardMaker software, and end-user must conform to these requirements. PIN Policy established also applies to PUK.		✓	✓
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 Manager software or Administrator in Sphinx CardMaker software, as required. Administrator can specify if end-user will be allowed to change this setting.	✓	✓	✓
Encryption	Each issued Sphinx card or Sphinx account is secured by its own unique set of TDES encryption keys. If an installation requires a specific encryption method, the modular Sphinx encryption engine can be exchanged for special customized versions.	✓	✓	✓
Secured data exchange with card	For card installations that store Sphinx data on the card, all security sensitive Sphinx data is first encrypted before being exchanged with the card.	✓	✓	✓
Card security features	Sphinx takes advantage of the card security features already offered by the powerful compatible card technologies to provide an additional layer of security. See Solution Packages at www.odsphinx.com.	✓	✓	✓
Secure web server	Sphinx CardMaker software, installed on a Windows 2000 Server or Windows 2003 Server machine, utilizes the Windows information server functionality and Secure Socket Layer (SSL) encryption to provide secure server functionality.		✓	✓
Connection to secure server protected by SSL	All security sensitive Sphinx data is first encrypted before being exchanged via SSL protected connection with the		✓	✓

protected by SSL	secure server.			

Other Software Features

Feature	Description	Sphinx Standalone	Sphinx Enterprise	Enterprise PKI
Wide compatibility	The Sphinx software can be used out-of-the-box with a broad diversity of RFID and contact chip cards, cards readers, and PKI applications. See www.odsphinx.com for Compatible Products list and out-of-the-box Solution Packages.	✓	✓	✓
Built for interoperability	The Sphinx software is built around open API standards to provide interoperability between platforms, card readers, cards, and third-party software solutions. Sphinx is either out-of-the-box compatible or can easily be integrated with many third-party software and hardware products. By leveraging interoperability standards, Sphinx reduces the total cost of ownership for the end customer. PC/SC: can be used with all PC/SC conforming smart card readers. ISO 7816: has built-in interfaces for a number of ISO 7816 compatible cards. ISO 7816 compatible cards that are currently not supported can easily be integrated with Sphinx. ISO 14443 A/B: supports ISO 14443 compatible RF cards through a number of contactless readers. ODBC: compatible with major database systems such as MS Access, MS SQL, Oracle, mySQL. LDAP: interfaces with LDAP-based directories such as Active Directory. COM: includes COM API for server and client-based software. XML: includes API based on XML-RPC function calls over IP.	✓	✓	✓
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 Manager 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 CardMaker API for third-party applications on server computer	Data elements of the Sphinx CardMaker database are accessible through standard ODBC API. CardMaker 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.		✓	✓

Open Domain Sphinx Solutions, Inc.
524 Union Street, Suite 209
San Francisco, CA 94133
Tel (415) 398-2310 Fax (415) 398-2396
info@odsphinx.com www.odsphinx.com