

Sphinx PKI Middleware



The Sphinx PKI middleware enables an ID card or token to support the full spectrum of certificate-based functions within a Public Key Infrastructure (PKI).

Full-featured flexibility

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.

The PKI middleware provides the interface to the card for certificate-based functions. Since the PKI middleware conforms with CSP and PKCS#11 industry standards, the PKI-enabled card or token can immediately be used with a large number of applications to perform critical security related functions, such as:

- Certificate-based logon to networks.
- Certificate-based VPN logon.
- Certificate-based authentication using Web-browsers.
- Certificate-based email encryption.
- Digital signature for documents.

The Sphinx Enterprise PKI version is compatible with a wide spectrum of smart cards, tokens and applications.

How do the Sphinx logon functions and the PKI middleware work together on one card?

With the Sphinx CardMaker software, cards are initialized for logon manager and PKI usage in a single step. The assigned default card PIN and PUK authenticate the user for both Sphinx Logon Manager and PKI functionality.

How do cardholders use the integrated software?

The PKI middleware is called "middleware" because it provides the interface between PKI-aware applications and the card, and end-users do not need to interact directly with this software. PKI-aware applications are configured independently of the Sphinx PKI middleware; the user simply presents his card to the reader and enters his PIN for authentication.

Windows logon choices

The Sphinx Enterprise PKI version provides two mechanisms for card enabled Windows logon:

Certificate-based logon: During logon, Windows accesses functions of PKI middleware to verify the certificate on the card, and the cardholder is logged on. This method provides the highest level of logon security: only cards with an authorized certificate can logon. Requires Public Key Infrastructure.

GINA-based logon: Provides standard Sphinx GINA-based Windows logon functionality where software transfers user name, password, and domain from the card to the Windows logon process.

Advantages

Having both logon to Windows mechanisms available on one card can offer the following advantages:

- Companies that require multiple domain logon profiles can save multiple GINA-based profiles in Sphinx, in addition to their certificate-based logon.
- Companies whose PKI environment is not accessible at all sites, or who require quicker logon speeds for frequently switching users, can use GINA-based logon for these users.
- Companies planning to migrate to a PKI infrastructure in the future can use the Sphinx GINA logon now and the certificate-based logon later, with no change to the card.

Sphinx PKI Middleware

Product advantages

See also additional information under Sphinx Enterprise PKI at www.odsphinx.com.

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, Vista, 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	Supports all major PKI/CA systems such as: Entrust, Microsoft, RSA, SafeLayer, Verisign.
Supported applications	PKCS#11/CryptoAPI applications such as: VPN: Check Point, Cisco, Microsoft, NCP. Secure e-mail clients: Microsoft Outlook (98, 2000, XP, Vista, Express), Novell Groupwise 6, Mozilla Thunderbird, Mozilla Firefox. SSL authentication for browsers: Microsoft Internet Explorer, Mozilla Firefox. Other applications: Citrix, Lotus Notes, PGP, SSH Tectia Client, RSA SecurID, SafeBoot, Utimaco.
Card options	Works out-of-the-box with a diversity of powerful cards and tokens. See Solution Packages at www.odsphinx.com
Proven	In continuous use at substantial installed base of government, financial, educational, and healthcare institutions world-wide.

System requirements

Operating system	On end-user computers: Windows 2000, 2003, XP, or Vista. On administrator computer: Windows XP, Vista, 2000 Server or 2003 Server.
Hardware	Pentium processor, 128 MB RAM, 8 GB disk space, or higher.
PKI infrastructure	Any supported PKI system and PKI-aware application listed above.
Browser	Internet Explorer 5.5+ or Firefox 2.0+.

Purchase information

Priced by end-user license. Includes all software components required to implement Sphinx solution.

Version	Order #	Description	Included software components
Sphinx Enterprise PKI	S-30-PKI	Provides built-in PKI card interface and middleware, to support certificate-based functions.	Sphinx Logon Manager, for end-user computers Sphinx CardMaker, for administrator computer PKI middleware, for all computers

