Theft of on-line passwords is the fastest-growing computer security threat
Symantec, Dec 2003

protectID
protectID

protectID$_{tm}$ USB tokens or ID cards - eliminate concerns with internet passwords

SENTRY^{PM}

MK-BR-00080802-5

protectID

product specification

Compatibility
Microsoft Internet Explorer
Microsoft Outlook, Outlook Express
Netscape Navigator
Netscape Messenger

protectID has been designed to comply with standard server, browser and email products to simplify the introduction of strong security to your current installations. No new user interfaces for complicated security settings, use your existing product training and documentation.

The supported standard interfaces mean that **protectID** can immediately replace components in e-commerce products, strengthening security now.

Product Features	
A drop-in replacement for passwords	Standard interfaces provide client-authenticated SSL which allows the protectID token to replace user or admin passwords and provide confidence about who is accessing or administering a service
Standards-based host changes	Most servers (Windows, Netscape, Apache etc) can be configured to support client-authenticated SSL
Standard key and certificate formats for loading	ProtectID accepts keys and certificates in the standard PEM format (as produced by OpenSSL etc)
Additional user benefits	Standard plug-ins support signed and encrypted email with Microsoft Outlook, Netscape Messenger and other email packages
Secure channel to token	Allows the option of remote administration of tokens for PIN reset and even key loading if required.
Key-generation on token	Optional key generation allows a key to be generated within the token and which never leaves the token – specified by some e-signature schemes (1,2)
1024bit RSA keys	Exceeds requirements for business transactions
Two user RSA key pairs	Separate authentication and confidentiality/encryption to allow key escrow of encryption keys without threatening the authentication key. Key escrow allows recovery of encrypted data even if the token is lost.
Card option	The protectID application can also be supplied in card format. For example, a photo-identity card, or a proximity card for physical access control.
Low-cost	Based on standard card operating systems (MULTOS and Javacard) allowing access to volume priced products. A small application size and optimised personalisation method gives low total cost (3)
Resistant to security attacks	The protectID application uses a number of techniques to protect the user PIN and user keys on the token from brute-force discovery attacks, power analysis and attempts to disturb application processing.

(1) 1024bit RSA key set typically generated in 60s. Contact Sentry if you require further technical information on key generation.
(2) ProtectID can be supplied on either the MULTOS or Javacard operating systems. The MULTOS operating system has been evaluated at the highest ITSEC E6 level and ensures that application data such as keys is confidential.
(3) Application size does depend on the number of certificates and other data that might be required by some custom solutions.

Please contact support@sentrypm.com for further information, pricing and lead-times.