

Pentio PKI USB Token™ 3500 SM



Windows
7/Vista
MacOS X

RSA
2048bit

持ち出しデータをAES256bitで暗号化 暗号フラッシュメモリを搭載したUSBトークン

RSA2048bit公開鍵暗号ICチップ搭載USBトークンに本体内部データをAES256bit共通鍵で自動暗号化する2GB/4GBフラッシュメモリを搭載。PKCS#11サポートにより、WindowsだけでなくMacOS Xにも対応

高性能なRISC 32bit CPUを搭載

Pentio PKI USB Token™ 3500 SMに内蔵するICチップは、高性能なRISC型 32bit CPUを採用し、高度な鍵処理にも耐えられる高速性能と、鍵処理の待ち時間低減によるレスポンスをご提供します。また、2048bit証明書を複数搭載できる62KB (Free) 大容量のEEPROMも搭載しております。

RSA2048bit公開鍵暗号*1、 AES256bit共通鍵暗号、 SHA2ハッシュ関数、 次世代暗号アルゴリズム搭載

Pentio PKI USB Token™ 3500 SMの内蔵ICチップは、長期間の利用で心配される暗号アルゴリズムの危殆化に対応できる「次世代暗号アルゴリズム」を採用し、「暗号2010年問題」などで心配される暗号強度にお応えします。RSA2048bit公開鍵暗号、AES256bit共通鍵暗号、SHA2ハッシュ関数をICチップで処理できます。



PKCS#11サポートにより、 WindowsだけでなくMacOS Xにも対応

Pentio PKI USB Token™ 3500 SMをWindows / Macでの利用は、PKCS#11でご提供するミドルウェアCSPを搭載することご利用いただけます。

Windows® 7, Windows® Vista, Windows® XP (SP2), Windows® 2000 (SP5), いずれも32bit OS対応のCSPです。MacOS X Leopard (10.5), Tiger (10.4) に対応したPKCS#11ドライバソフトウェアをご提供可能です。

USBデバイスに大容量の暗号化・ 復号メモリ搭載、内部でAES256bit 暗号化・復号処理を実現

Pentio PKI USB Token™ 3500 SMは、2GBまたは4GBの大容量メモリを搭載しています。また、このデバイスメモリへの書き込みには強度の高いAES256bitの暗号化処理をデバイス内部のハードウェアで実現、同時に読み出しにもAES256bitで復号処理。デバイス内部でのハードウェア処理により、たいへん高速で安全性の高い暗号化・復号をご提供します。これにより重要文書・データの漏洩防止をサポートします。

大容量の暗号化・復号処理ソフトウェアは USBデバイス内部に格納・自動搭載

Pentio PKI USB Token™ 3500 SMは、暗号化・復号処理に必要なソフトウェアは、USBデバイス内部に格納しており、PC挿入時に自動的に搭載されます。

スマートカード技術による 安心の暗号キー作成メカニズム

Pentio PKI USB Token™ 3500 SMはスマートカード技術によってオンボードで安全な公開鍵と秘密鍵を作成し格納できます。

動作中でも抜き差し可能

Pentio PKI USB Token™ 3500 SMは動作中のPCでもUSBポートに抜き差し可能です。

優れた携帯性

Pentio PKI USB Token™ 3500 SMは長さ75mm・幅25mm・奥行14mm、重さはわずか48.2グラムなので、簡単に電子証明書を携帯することができます。

FIPS 140-2*2 Level3, セキュリティ認定モジュール搭載

Pentio PKI USB Token™ 3500 SMFの接触型ICチップは、暗号モジュールに関するセキュリティ要件の仕様を規定する米国連邦標準規格であるFIPS (Federal Information Processing Standards Publication) 140-2のレベル3に認定された非常に信頼性の高いチップです。FIPS 140-2 Level3認定モデル Pentio PKI USB Token™ 3500SMF は、2010年7月にモデル終了となりました。



*1 米国立標準技術研究所 (NIST) は、暗号解読研究の動向やコンピュータの処理能力の向上といった要因を考慮した上で、2010年以降はRSA公開鍵暗号方式において、これまでの1024ビットから2048ビットへの移行を推奨しています。日本でも2048ビットへの対応が進むことが予想されています。

*2 FIPS 140 (Federal Information Processing Standards Publication 140) -2暗号モジュールに関するセキュリティ要件の仕様を規定する米国連邦標準規格である。規格の最新版は2001年5月25日発行のFIPS 140-2である。

製品主要要件比較表

	1500	2100	3100	3300	3500SM
高性能CPU	—	—	○ 16bit	◎ 32bit RISC	◎ 32bit RISC
セキュリティ認定	—	○ FIPS140-2 L2	○ FIPS140-2 L3	◎ FIPS140-2 L3 CC EAL5+	—
Microsoft BaseCSP対応	—	—	—	○ BaseCSPv5-v7 Minidriver対応	—
ミドルウェア 自動インストール	× 手動	× 手動	× 手動	△ Server2008R2, Windows7, Server2008, Vista,自動認識	× 手動
PKCS#11対応	○ Windows対応	○ Windows対応	○ Windows対応	◎ MacOS, Linux, Windows対応	○ MacOS X(10.4, 10.5) Windows対応
公開鍵暗号鍵長	○ RSA 1024bit対応	○ RSA 1024bit対応	◎ RSA 2048bit対応	◎ RSA 2048bit対応	◎ RSA 2048bit対応
64bit OS 対応	—	○ Vista, Windows7	○ Vista, Windows7	◎ Vista, 2008, Windows7, 2008R2, Unix, Linux	× 32bitのみ
大容量メモリ					◎ (2GB/4GB) ハードウェアでAES256bit 暗号化・復号メモリ

▶ Pentio PKI USB Token™ 3500 SM 仕様・価格

型式	PUB-3564SM2	PUB-3564SM4
ホストインターフェース	HID (Human Interface Device)	
証明書と標準化対応	PKCS#11, PKCS#12, MS CAPI, PC/SC, X.509 v3 Certificate Storage, SSL v3, IPSec/IKE, ISO 7816 1-5	
チップ	32bit	
メモリ	62KB(Free)	
アルゴリズム	RSA2048, DES, 3DES, AES, HMAC, SHA1, SHA2	
セキュリティ認証	なし	
Microsoft Base CSP	なし	
PKCS#11	Windows 7, Windows Vista, Windows XP (SP2), Windows 2000 (SP5)、各32bit OS MacOS X (10.5, 10.4)、各intel版のみ ※Linuxなし	
メモリ容量	SLC 2GB	SLC 4GB
USB	USB 2.0 high speed 480 Mbps	
読み出し/書き込み	読み出し 30MB/s以上、書き込み 22MB/s以上	
暗号化	Native 256bit AES ハードウェア暗号、Chain Block Cipher mode	
大きさ、重さ	75 x 25 x 14 mm、48.2g	
価格	オープン価格	オープン価格

代表的な連携ソリューション

Webサイト認証 Apache/IIS

代表的なWebサーバであるApacheとIISでのアクセス認証ができます。

業務サーバ/グループウェア認証(SSO)

リバースプロキシ型シングルサインオン(SSO)との組み合わせで、グループウェアや複数の業務サーバへのアクセス認証を、1回の証明書(秘密鍵)認証でできるようになります。

ネットワークストレージ認証(WebDAV)

PCのブラウザからWebサーバ上のファイルやフォルダを簡単にアップロード/ダウンロードできるWebDAVで、PKI証明書によるアクセス認証を実施できます。

リモートアクセス認証
FirePassシリーズ

SSL-VPNアプリケーションとの組み合わせで、セキュアなリモートアクセスが可能になります。



無線LAN認証
Enterpas Std

RADIUSサーバとの組み合わせで、強固で使い勝手のよい無線LAN認証基盤を構築できます。



PDF文書電子署名
Adobe® Acrobat®

PDF文書作成時にPKI証明書(秘密鍵)を用いて、デジタル署名を利用できます。



ペンティオ株式会社

[PKIソリューション事業部]

〒160-0004 東京都新宿区四谷2-4 久保ビル3F

Tel.03-5919-0971 Fax.03-5919-0980 <http://www.pentio.com/>

2010年7月