

Pentio PKI IC Card™ 3300C



※ 白無地でのご提供になりますので、お客様が自由にデザイン可能です。



Microsoft® Minidriver対応 Windows® 7, Vista, Server 2008標準搭載 2048bit RSA暗号に対応した次世代ICカード

Pentio PKI ICカード 3300Cは、次世代に求められる 2048bit RSA暗号、SHA256bit ハッシュ関数を処理可能なICカードです。マイクロソフト社のMinidriverに対応しており、Windows® 7, Vista, Server 2008ではミドルウェアソフトウェアはOSに標準バンドルされており、ドライバソフトウェアの配布などをシステム管理者から解放します。

高性能なRISC 32bit CPUを搭載

Pentio PKI ICカード™ 3300Cの接触型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、 SHA256bitハッシュ関数、 次世代暗号アルゴリズム搭載

Pentio PKI ICカード™ 3300Cの接触型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、SHA256bitハッシュ関数をICチップで処理できます。

FIPS140-2※2 Level3, Common Criteria EAL5+ セキュリティ認定モジュール搭載

Pentio PKI ICカード™ 3300C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。



※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。

Microsoft® Minidriver に対応、 Windows® 7, Vista, Server 2008 OS標準搭載

Pentio PKI ICカード™ 3300Cを利用するミドルウェアソフトウェアは、近年のWindows環境においては自動搭載/標準搭載されておりすぐに使い始めることができます。これによりシステム管理者は、ICカードのミドルウェアを配布から解放されコンピュータシステムのTCO軽減に貢献します。コンシューマ/一般ユーザー向けサービス用ICカードとしてもご利用いただけます。

Windows® 7, Windows® Vista, Windows® Server 2008に標準搭載されております。Windows® XPではMicrosoft社Webサイトより入手できます。

PKCS#11サポートにより、 MacOS X, RedHat, Debian, Ubuntu, Solaris にも対応

Pentio PKI ICカード™ 3300CをMac/Linuxでの利用は、PKCS#11でご提供するミドルウェアを搭載することでご利用いただけます。MacOS X, RedHat Linux, Suse Linux, Debian, Ubuntu Linux, Solaris などご利用いただけるPKCS#11ドライバソフトウェアをご提供可能です。

▶ ICカードリーダー/ライター

▶ OMNIKEY CardMan® 3121



低価格な接触型リーダー/ライターです。

▶ ご利用可能なPentio PKI IC Card™

Pentio PKI IC Card™ 2300, 2400FIPS, 2500DI, 2600FC, 3300C

▶ インターフェース

USB1.1/2.0

▶ PC/SCドライバサポート

Microsoft® Windows® 98, ME, 2000, XP, Vista™, 7, CE3.0, Linux®, Mac OS® X

▶ 価格

6,300円(税込)

▶ OMNIKEY CardMan® 4040



PCMCIA接触型インターフェースによるリーダー/ライターです。

▶ ご利用可能なPentio PKI IC Card™

Pentio PKI IC Card™ 2300, 2400FIPS, 2500DI, 2600FC, 3300C

▶ インターフェース

PCMCIA

▶ PC/SCドライバサポート

Microsoft® Windows® 98, ME, 2000, XP, Vista™, 7, CE3.0, Linux®, Mac OS® X

▶ 価格

10,500円(税込)

▶ Gemalto USB-TR



安価で高性能なUSB接続ICカードリーダー

▶ ご利用可能なPentio PKI IC Card™

Pentio PKI IC Card™ 2300, 2400FIPS, 2600FC, 3300C

▶ インターフェース

USB2.0フルスピード (12Mbps)

▶ PC/SCドライバサポート

Microsoft® Windows® 95, 98, ME, NT4, 2000, XP, Server2008, Vista, 7, CE5.0, MacOSX, Linux, Solaris

▶ 価格

オープン価格(スタンドはオプション)

▶ 補足表

	2300	2400FIPS	2600FC	3300C
高性能CPU	—	—	—	◎ 32bit RISC
セキュリティ認定	—	○ FIPS140-2 L2	○ FIPS140-2 L2	◎ FIPS140-2 L3 CC EAL5+
Microsoft Minidriver対応	—	—	—	○ BaseCSP Windows対応
BaseCSPミドルウェア自動搭載	× 手動	× 手動	× 手動	△ Windows 7, Windows Vista, Windows Server 2008標準搭載 WindowsXPでは手動搭載
PKCS#11対応	○ Windows対応	○ Windows対応	○ Windows対応	◎ MacOS, Linux, Windows対応
公開鍵暗号鍵長	○ RSA 1024bit対応	○ RSA 1024bit対応	○ RSA 1024bit対応	◎ RSA 2048bit対応
非接触利用			○ FeliCa対応	▲ オプション対応

▶ プライベート認証局パッケージについて

用途に応じて最適な証明書を発行し、
多様なPKI認証ソリューションと提携

プライベート認証局(プライベートCA)は、インターネットで利用されるPKI証明書を発行する発行局と証明書を認証する認証局です。公開鍵を配布するリポジトリもあわせて提供します。世界標準X.509準拠の証明書認証方式により、インターネット通信時の「盗聴」「データ改ざん」「ユーザのなりすまし」などを防ぐようになります。

プライベート認証局(プライベート CA)



▶ Pentio PKI IC Card™ 3300C 仕様・価格

型式	PIC-3364
通信方式	接触 (T=0)
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、AES256、SHA1、SHA256、MD5、MMAC
セキュリティ認証	FIPS140-2 Level3 Common Criteria EAL5+(chip)
Microsoft Base CSP	Windows 7、Windows Server 2008 R2、Windows Vista、Windows Server 2008 Windows XP、Windows Server 2003
PKCS#11	Windows各種 MacOS X Linux (Red Hat Linux、SUSE Linux、Debian、Ubuntu) Sun Unix (Solaris)
非接触部	(オプション)MIFARE、HID、FeliCa
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アプライアンスとの組み合わせで、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

Enterpris 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6月