

Pentio PKI USB Token™ 3300



写真は原寸大です。



Windows®XP / Vista / Windows®7で ドライバの自動インストールを実現

Pentio PKI USB Token™シリーズは、ペンティオがお客様にご提供するPKI認証ソリューションでのご利用に最適なUSBトークンです。「Pentio PKI USB Token™ 3300」のドライバは、新たなソフトウェアやミドルウェアを追加する必要がなく、企業や組織内で簡単に展開し、シームレスに利用することができます。

Microsoft®Windows® XP/Vista/7で ドライバの自動インストールを実現

Windows Vista™ではミドルウェア・ドライバが搭載済みであり、『Pentio PKI USB Token™ 3300』をPCに挿すだけですぐに利用が可能な自動インストールを実現しています。

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 USB Token™ 3300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。

FIPS140-2² Level3, Common Criteria EAL5+ セキュリティ認定モジュール搭載

Pentio PKI USB Token™ 3300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。



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

Pentio PKI USB Token™ 3300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、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 USB Token™ 3300をMac/Linuxでの利用は、PKCS#11で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カード発行サービスによる 大量発行可能(オプション)

Pentioトークン3300は、トークン内容にICカード (SIM形状) を格納する構造です。その為ICカード発行機能を使用し、連続的に大量発行サービスすることが可能です。ICカード発行サービスは別途有償オプションとなります。

▶ 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™ 3300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™ 3300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™ 3300は長さ64mm・幅16mm・奥行8mm、重さはわずか9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。

1 米国標準技術研究所 (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。

