



## LYNKS™ Series II HSM



### 小型高性能HSM (Hardware Security Module)

- USB 及び PCMCIA ハウジング実装 HSM
- 最新の高速度 Suite B 暗号アルゴリズム対応  
(ECMQV 及び EC-DH 鍵設定を使用した楕円曲線暗号, AES, SHA-2)
- \* LYNKS シリーズは CA, RA 局の暗号鍵管理と鍵のリカバリー機能を低コストで提供
- \* Suite B 暗号アルゴリズムは米国政府、企業用途に機密情報保護に寄与
- \* ファームウェアのセキュア更新可能 (アルゴリズム、機能の選択可能)
- \* 多数のアルゴリズムからの選択可能
- \* 米国政府使用の FORTEZZA サポート

### 特長

最高峰のランダム番号発生と鍵生成機能
FIPS-140-2 レベル2
FIPS 140-2 Level 3 認定最終処理中 (2008.4現在)
ユーザープライベート鍵へのアクセスは PIN が必要
抗タンパー、タンパー検知
タイムスタンプ機能 (購入時オプション)
Microsoft 暗号 AP I(MSCAPI)のアプリケーション、カード、PKCS#11 をサポート
Windows 2000, XP, Server 2003 用 WLQL 認定ドライバーの提供
米国政府 Jumbo FORTEZZA のサポート (128 個の証明書を保持可能)
AES, SHA-2 の暗号化ハードウェアアクセラレータ



### ICH

正規一次代理店  
 株式会社アイシーエイチ  
 東京都品川区西五反田 3-5-17-408  
 TEL: 03-3432-3336  
 e-mail: [ich-support@ich-one.com](mailto:ich-support@ich-one.com)  
<http://www.ich-one.com>



SECURITY TO THE EDGE™



## 仕様

### 対応暗号アルゴリズム

RSA 1024, RSA 2048, DSA 1024 (デジタル署名、鍵交換アルゴリズム)  
SHA-1, MD5, SHA-224/256/384/512 (セキュアハッシュアルゴリズム; HMACC /SHA-1)  
DES, two & three-key triple DES with ECB, CBC  
KEA Key Exchange 1024 exchanges 80-bit SKIPJACK key  
(AES) 128/192/256 ECB, CBC, OFB, CTR, and key wrap modes  
楕円曲線暗号(ECC)、NIST curves in GF(p) (P-256, P-384, and P-521)  
ECMQV及び ECDH鍵設定(NIST SP 800-56A Key Guidelines)  
ECDSAデジタル署名アルゴリズム

### インターフェース

PCMCIA 2.1  
USB 2.0, 1.1

### 認証

FIPS 140-2 Level 2 with Physical Level 2 and Level 3 option

### 定格

稼働電圧: Vcc = 5VDC ± 5%  
消費電力: <1W (平均)  
7年以上保存保証のリチウム電池

### 環境条件

動作温度範囲: 0 ~ 55  
保存温度範囲: -20 ~ 65  
動作湿度: 最大90% (結露なきこと)  
PCMCIAの取扱: 振動、ショック、曲げ、擦れ、落下の無き事

### 標準対応

- Microsoft WHQL-certified drivers
- Microsoft CryptoAPI, Microsoft Card Module and PKCS #11 interoperability
- FIPS PUB 46 Data Encryption Standard
- FIPS PUB 180-2 Secure Hash Algorithm Standard
- FIPS PUB 186-2 Digital Signature Standard
- FIPS PUB 197 Advanced Encryption Standard
- SP 800-38A Block Modes of Operation
- FCC Class B certification and CE Mark Certification



ICH

正規一次代理店  
株式会社アイシーエイチ  
東京都品川区西五反田 3-5-17-408  
TEL: 03-3432-3336  
e-mail: [ich-support@ich-one.com](mailto:ich-support@ich-one.com)  
<http://www.ich-one.com>