CipherTools™ enables developers to create or enhance business applications to make optimal use of the high assurance features offered by Thales nShield hardware security modules (HSMs). Empowering customers to exercise full control over the use of cryptography in their organization, CipherTools is specifically designed to facilitate the development of software applications that run in cloud, server or workstation environments, enabling them to deliver secure key management for sensitive private keys, increased cryptographic processing performance, scalability, and fail-over resilience.

**Key Benefits**
- Maximizes developer productivity through easily compiled sample code and detailed documentation
- Enables developers to choose between industry standard and Thales specific APIs
- Allows vulnerable software-based encryption implementations to use tamper resistant nShield HSMs
- Enables scalable lifecycle management of key material and facilitates failover and disaster recovery using the Thales Security World key management architecture
- Interoperates with wide range of hardware and operating systems, enabling key material used by host-side applications to be platform independent and transportable
**Thales e-Security CipherTools™**

**TECHNICAL SPECIFICATIONS***

<table>
<thead>
<tr>
<th>Industry Standard APIs</th>
<th>Application</th>
<th>Key Types</th>
<th>Security Policy</th>
</tr>
</thead>
<tbody>
<tr>
<td>PKCS#11</td>
<td>Using PKCS#11</td>
<td>All nShield supported key types except El-Gamal</td>
<td>Subset of Security World features mapped onto industry standard API</td>
</tr>
<tr>
<td>Microsoft Crypto API/CNG</td>
<td>Using Microsoft CryptoAPI/CNG</td>
<td>CryptoAPI: RSA, DSA, DH CNG: RSA, DSA, ECDSA, DH, ECDH</td>
<td></td>
</tr>
<tr>
<td>Java/JCE</td>
<td>Using Java/JCE</td>
<td>RSA, DSA, 3DES, AES</td>
<td></td>
</tr>
<tr>
<td>OpenSSL</td>
<td>Using OpenSSL and CHIL engine</td>
<td>RSA, DSA, DH</td>
<td>Security World features and policies supported</td>
</tr>
<tr>
<td>nCore</td>
<td>Using custom C or Java</td>
<td>All nShield supported key types</td>
<td>Security World features and policies supported – fully custom security policies possible</td>
</tr>
</tbody>
</table>

**Compatibility and Licensing**
- Compatible with all nShield HSMs
- Licensed on a developer seat basis
- Allows unlimited/license-free nShield enhanced applications to be created

**Toolkit Contents**
- Software to install on Unix or Windows platform
- Thales libraries (header files, sample code and documentation)
- Full details of Thales vendor extensions
- Cryptographic hardware interface library
- Microsoft CryptoAPI/CNG
- Thales Java/JCE plus Java documentation and sample code
- Crypto API guide
- nCore developer tutorial
- Developer samples kit and tutorials
- Additional C and Java libraries for developers use

**Supported Algorithms**
- Asymmetric public key ciphers
  - RSA (1024, 2048, 4096), Diffie-Hellman, DSA, El-Gamal, KCDSA, ECDSA, ECDH
- Symmetric ciphers
  - AES, ARIA, Camellia, CAST, DES, RIPEMD160 HMAC, SEED, Triple DES
- Hash Functions
  - SHA-1, SHA-2 (224, 256, 384, 512 bit)
- Full Suite B implementation
- Fully licensed Elliptic Curve Cryptography (ECC) (Including Brainpool and custom curves)

**Supported OS Platforms**
- Windows
- Linux (Red Hat and SUSE)
- Solaris
- IBM AIX
- HP-UX

**Target Hardware**
- All nShield models
  - nShield Solo
  - nShield Connect
  - nShield Edge (Windows only)
- Performance (signatures/second)
  - Up to 6,000 (RSA)
  - Up to 2,400 (ECC)
- Supported interfaces
  - PCI/PCle, Ethernet, and USB
- Backup resiliency by adding multiple HSMs
- Unlimited key storage via Security World key management architecture

**Professional Service Offerings**
- Expert developer support
- Developer training
- Design assistance
- Code Review
- Custom application development

Follow us on: