Today, cryptographic keys are the cornerstone of any protection scheme. They are used to protect digital property, including media, software, and devices. Keys are also employed to encrypt user licenses, bind devices, prove identity, and secure communications against eavesdroppers. Keys are therefore a critical component of data, application, and system security.

**Prevent discovery and abuse of critical keys used to:**
- Encrypt user-bound content, media, and software licenses
- Sign digital documents and application code
- Prove identity and secure session keys in e-commerce and authentication
- Protect Host Card Emulation (HCE) Keys

**Protect Your Keys**
Access to digital content, data, and information systems is commonly protected by encryption, a first line of defense to protect against piracy and theft. However, the single point of failure remains the instance at which the decryption key is used. This point is easily identifiable through signature patterns and cryptographic routines. Once found, an attacker can easily navigate to where the keys will be constructed in memory. Subsequently, fatal exploits can be easily created.

Arxan’s TransformIT technology, based on White Box Cryptography (WBC), combines mathematical algorithm transformations with data and code obfuscation techniques to transform the key and related operations so that the key cannot be discovered. The keys are never present in their original form, in either the static application or in runtime memory.

TransformIT works by separating application data into two domains: the Open Domain and the Encrypted Domain. The open domain is data that is completely viewable by attackers viewing the static or dynamic data present in an application. All code and data in the open domain can be understood by attackers.

The Encrypted Domain encompasses data and code protected by TransformIT. From the attacker’s point of view, there is no way to meaningfully interpret the data in the encrypted domain. All data and keys operated on by TransformIT remain in the Encrypted Domain. This includes static keys, dynamic keys, and any sensitive user data.
TransformIT®

Core Features and Benefits of TransformIT

- **Algorithmically Strong** – Proven approach is fundamentally secure and resistant to known attacks on White Box Cryptography implementations
- **Performance Friendly** – Performance vs. security tradeoffs are fully tunable
- **Easy to Use** – Simple API allows easy integration with application
- **Portable** – Source code-based implementation is portable to all platforms and compatible with any application hardening technique
- **Secure** – Self consistency checks provide defense-in-depth security and high resistance to attacks

<table>
<thead>
<tr>
<th>TransformIT Features</th>
<th>TransformIT Benefits</th>
</tr>
</thead>
<tbody>
<tr>
<td>Effectively Hides Keys</td>
<td>Actual key bits never form in memory nor registers. By preventing the cryptographic keys from ever appearing, memory dump and memory remnants attacks are thwarted.</td>
</tr>
<tr>
<td>Actively Prevents Key Discovery</td>
<td>By using internal data consistency checks, data injection attacks are prevented.</td>
</tr>
<tr>
<td>Encrypted Domain Operations</td>
<td>Data is operated on within the encrypted domain, so operations can be performed on data without ever having to decrypt and reveal the sensitive keys or data.</td>
</tr>
<tr>
<td>Tunable</td>
<td>Different methods of key protection are available, allowing a tradeoff between size/performance constraints and level of security.</td>
</tr>
<tr>
<td>Data Obfuscation</td>
<td>Sensitive application data can be processed and operated on without being decrypted.</td>
</tr>
</tbody>
</table>

**Best Practice: For Maximum Security, Implement TransformIT with Code Hardening**

Implement a layer of defense around the Encrypted Domain by hardening programmatic elements such as WBC implementations to protect against code lifting. GuardIT® and EnsureIT™ are Arxan’s application hardening products which prevent tampering, reverse engineering and piracy of software. Critical functions of an application’s binary are protected through patented Guard technology. Guards are tiny security units that protect the application and each other in three ways:

- **Defend against reverse engineering, tampering and any manner of theft.**
- **Detect an attempted attack on the application code, or on another Guard.**
- **React in standard ways such as safely exiting or programmatically customized ways.**

As an application becomes subject to hacking, Guards are triggered which then activate custom or standard reactions such as key erasure, forced re-activation or traitor tracing, even before the hacker can compromise the application. Together, these technologies provide the strongest, most performance-efficient and cost-effective software protection available today.

**TransformIT® Specifications**

- **Supported Algorithms**
  - AES – Encryption and decryption for ECB, CBC, GCM and CTR modes, Sign, Verify
  - RSA – Encrypt, Decrypt, Sign, Verify
  - ECC – ECDH, ECDSA, ElGamal Decryption
  - DES, 3DES – Encryption and Decryption
  - SHA – Cryptographic Hash
  - MAC - CMAC (AES) and HMAC (SHA)
  - KDF - OMA, CMLA and NIST
  - DH – ECDH and FFDH

- **Supported Platforms**
  - Linux, Mac OS X, Windows, Android, Apple iOS, Chrome OS

- **Supported Key Scenarios**
  - Static – Build/Compilation time keys
  - Dynamic – Runtime generated keys