DATA SHEET

CipherKnight™ White-box

Software based security solution

BUSINESS ADVANTAGES

- **CipherKnight™** implements standard cryptographic algorithms in a white-box format, ensuring that keys and data remain secure during cryptographic operations. It also allows users to chain multiple ciphers or create custom key derivation mechanisms, providing flexibility and enhanced security.

Highlighted Features

- **Key protection** offers comprehensive security, defending against key-lifting attacks that commonly target IoT-connected devices.
- **Generating true random number (TRNG)** securely within a white-box environment. Historically, this feature was only available in hardware, but by implementing it in software, we enhance security algorithms while reducing bill of materials (BOM) costs.
- **White-box chaining** allows multiple white-boxes to be combined for derived keys, using ciphers like ECC and AES. This creates a more secure and flexible solution compared to single-link cipher solution.
- **White-box node-locking** uses unique fingerprinting from the targeted device to bind the white-box code and keys to that specific device, effectively preventing cloning attacks.
- **Custom Key Derivation Function (KDF)** in a white-box environment allows users to incorporate their own "secret sauce" into the KDF, adding extra layers of security while building white-box ciphers.
- **Updateable software solution** – Connected devices can receive updates to address new threats or attack vectors. In contrast, updating comparable hardware solutions is often significantly more costly and complex.

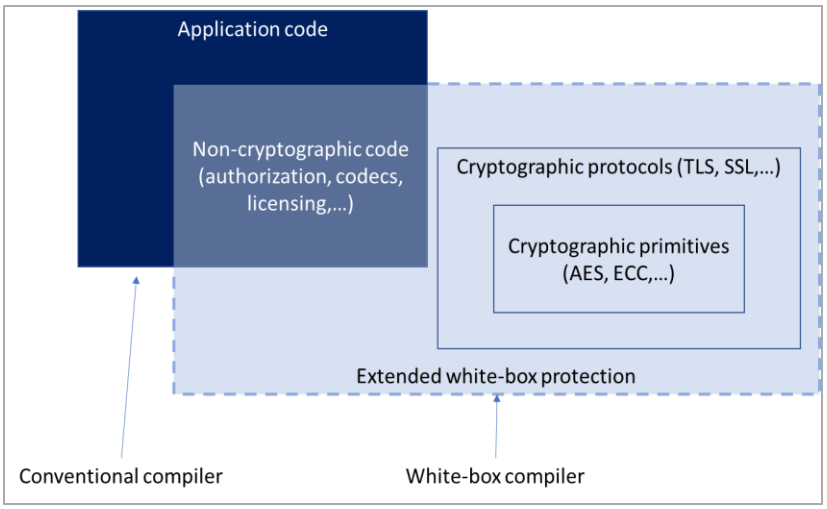
The ever-evolving attack vectors targeting modern IoT devices require a dynamic solution that can react quickly to new threats without a change in hardware.

CipherKnight™ provides protection necessary to deter and defend against a broad range of attacks targeting the software application layers. Our solution implements the defenses needed to protect existing keys and cryptographic operations of any connected devices in the absences of dedicated hardware security.

Protect the vulnerable devices at the edge of the network.

- Devices at the edge of sensing networks and IoT-connected jobsites often lack high-grade security, making them prime targets for malicious actors..
- Our white-box solution provides sufficient security for these devices by allowing them to perform cryptographic operations securely.
- CommScope CipherKnight™ can be seamlessly updated over a network connection, ensuring continuous protection for applications and keys in the field.

CipherKnight Primitive Integration Example Diagram



Contact the CommScope ANS Security Team for product information and sales:

- knightlicense@commscope.com
- United States: 888-944-4357
- International: +1-215-323-2345

CipherKnight™ Specifications and Minimum Requirements

white-box Algorithm	Description
AES 128, 256	CBC, CCM, CMAC, CTR, ECB, GCM, KeyGen
CSPRNG	CTR-DRBG
DH 2048	Key Agreement, KeyGen
ECC 256, 384, 521	Sign, Verify, Key Agreement, KeyGen
RSA 2048, 4096	Encrypt, Decrypt, Sign, Verify, Key Agreement, OAEP, KeyGen
SHA 256, 384, 512	Hash, HMAC, HKDF, PRF
TRNG	White-box true random number generator

Minimum Memory Requirements	
CipherKnight white-box	130KB on typical IoT device
	C/C++ source code generation with no specific target dependency
	Configurable to create only white-boxes that are needed

CPU Minimum Requirements	
CipherKnight white-box	None

ORDERING INFORMATION

Part Number	Description
903100-000-00	CipherKnight white-box Software License

Contact the CommScope ANS Security Team for product information and sales:

- knightlicense@commscope.com
- United States: 888-944-4357
- International: +1-215-323-2345

COMMSCOPE®

Note: Specifications are subject to change without notice.