Secure Networks

Cybersecurity

WiZ-Knight

USB Powered IP Encryptor

WiZ-Knight is a USB powered IP encryptor dongle that enables the user to leverage on public Ethernet/ IP infrastructure to connect to multiple sites in a secure manner. It employs AES algorithms for data confidentiality, Secure Hash Algorithm (SHA) for integrity protection as well as Internet Key Exchange (IKE) protocols for keys derivations and authentications.

The remarkable characteristic of WiZ-Knight lies in its mobility/small size which enable it to be carried anywhere easily. Its convenience is further extended by its WiFi capability, which enable it to connect to public access networks where registration is required, e.g. Hotel, Airport network.

WiZ-Knight is interoperable with NetCrypt series of IP encryptor, allowing user to form a secure VPN tunnel between the corporate HQ and remote client.

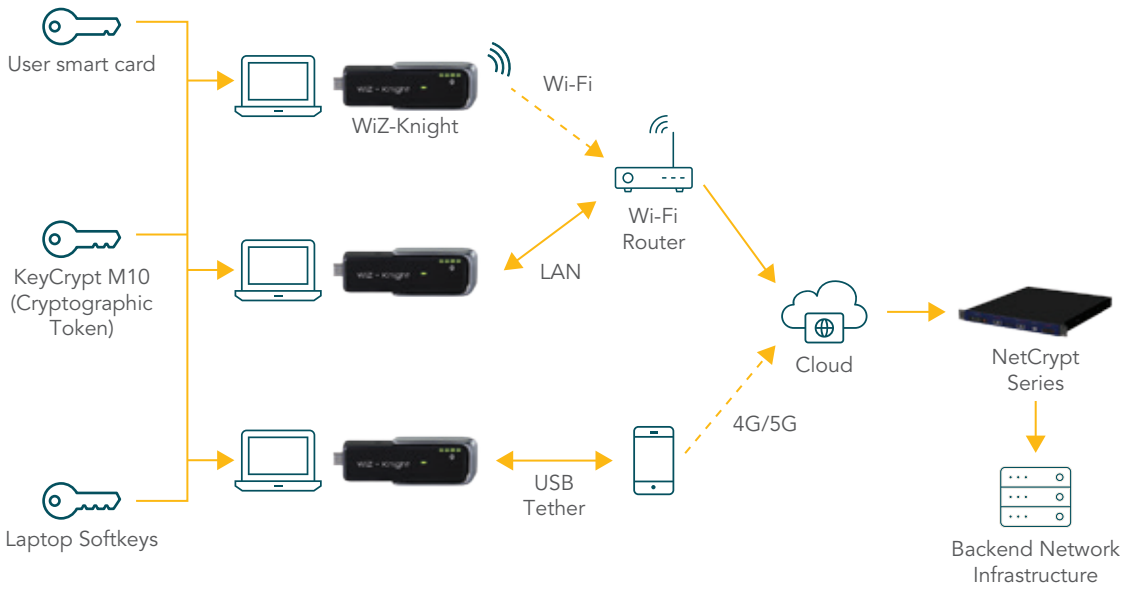
With the user login application installed at user's PC, it allows 2-factor authentication login to WiZ-Knight for usage upon successful identity authentication before it is able to unlock WiZ-Knight for secure tunnel establishment.

Key Features

- USB powered IP encryptor dongle
- Supports Wifi/LAN connections
- 20 Mbps throughput aggregate
- Supports AES algorithm for data confidentiality
- Supports 2 concurrent IPSec tunnels
- Suitable for Public Networks requiring Registration
- Support Multi-Authentication Softkey or cryptographic Smartcard

ST Engineering

Deployment Scenarios



Specifications

Network Interfaces	USB Type-C connector
Networking Features & Protocols	IP Security/Encapsulating Security Protocol Support Layer 3 encryption Traffic flow confidentiality
Authentication	RSA Public Key Signature (2048 bit)
Key Management	Support Internet Key exchange (IKE v2) DH supports up to 4096 bit Supports ECDH (up to P-521 bit) Group Transport Protection: The device has the option of providing confidentiality and data integrity protection to all key exchange traffic including the initial key exchange traffic
Encryption Algorithm/Modes	AES-CBC (256 bit)
Hash Algorithm	HMAC-SHA2 (256, 384, 512 bit)
Performance	Zero-loss encrypted throughput up to 20 Mbps (depending on IP packet size and used encryption mode) Support 2 concurrent IPSec tunnels
Management	
Security/Configuration	Audit logging
Physical Characteristics	Type-C model: 90mm (L) x 29mm (W) x 14.5mm (H)
Environmental	Storage Temperature: -20°C to 70°C Operating Temperature: 0°C to 40°C Humidity: Relative 10% -95%, non-condensing
Regulatory	EMC/EMI: FCC Part 15 Class B
Optional Feature	Supports customised algorithm loading feature

www.stengg.com/cybersecurity
cybersecurity@stengg.com