EtherCrypt U1000 is a layer-2 encryptor that protects the transmission of sensitive data over 1Gbps Ethernet and Metro-Ethernet networks. It offers full duplex encryption up to 1Gbps using the AES-256 algorithm, and is suitable for point-to-point, point-to-multipoint and fully-meshed Ethernet networks.

It can be easily deployed into existing networks without any changes to the network configuration and supports unicast, multicast and broadcast Ethernet frames. Designed to the strictest security standards, EtherCrypt U1000 includes a tamper-resistant chassis, emergency erasure and active zeroization. It also incorporates a FIPS 140-2 level 3 certified secure platform module – TrustCrypt for secure key storage and cryptographic processing.

Key Features
- High-assurance encryptor
- 1Gbps throughout
- Over Temperature Detection
- Emergency Erasure Button
Deployment Use Cases

Specifications

<table>
<thead>
<tr>
<th>Performance</th>
<th>Full duplex operation at speeds up to 1Gbps</th>
</tr>
</thead>
</table>
| Network Interfaces | Network: Ethernet II, IEEE 802.3  
Gigabit Ethernet ports with SFP interface (single mode, multi mode and copper) |
| Cryptography | AES 256 CFB mode  
Supports customized algorithm |
| Key Management | DigiSAFE proprietary key management  
Parameter loading using smartcard  
Automatic and transparent session key negotiation |
| Device Management | Local console port (9 pins D serial port)  
100 Base-T RJ45 Ethernet port – for remote monitoring  
SNMP V2c (operates with standard SNMP network management station) |
| Physical Security | Emergency erasure function  
Tamper resistant chassis  
Active zeroization of cryptographic data upon tamper detection  
User PIN protected Front Panel Menu |
| Operating Environment | Operating Temperature: 0°C to 40°C  
Relative Humidity: 0 to 90%  
Storage Temperature: -20°C to 65°C  
Meets FCC Part 15, Class B EMI/RFI requirements |
| Physical Characteristics | Tamper resistant chassis  
Tamper detection and response (FIPS 140-2 Level 3)  
Active zeroization of cryptographic data upon tamper detection  
User PIN protected front panel menu  
High temperature detection  
Emergency erasure button |
| Networking Features & Protocols | Supports Ethernet Layer 2 encryption  
Point-to-point, point-to-multipoint, multipoint-to-multipoint meshed networks  
Unicast, multicast and broadcast Ethernet frames |
| Security/Configuration | Automated power-up self tests  
Alarm/Audit log messages stored in memory with date and time  
LED indicators for link status monitoring  
Front Panel Menu-driven setup  
Battery Backup of cryptographic variables |
| Accreditation | DigiSAFE TrustCrypt – FIPS 140-2 level 3 certified cryptographic module (certificate #1304) |

Optional

| Key Management System (KMS) | Windows-based software system for key exchange parameter generation |
| Smartcard | Configuration card for user authentication and cryptographic key parameters |
| Feature | Supports customized algorithm loading feature |

ST Engineering Electronics Ltd.  
www.stengg.com/cybersecurity  
mktg.infosec@stengg.com

© 2019 ST Engineering Electronics Ltd. All rights reserved.