

DigiSAFE TrustCrypt

- Secure Platform Module

The DigiSAFE TrustCrypt is a multi-chip embedded cryptographic module certified to FIPS 140-2 level 3 (Certificate #1304).

TrustCrypt is a programmable cryptographic module designed to support high assurance applications and provide secure cryptographic resources, including secure key generation and storage. It is built upon a secure physical enclosure and contains a secure bootstrap which authenticates application loading.

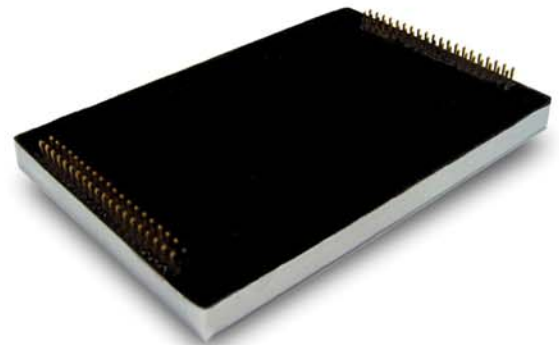
The module served as a secure platform for the range of DigiSAFE brand network security appliances. The network security appliances include WAN link Encryptor and IP Encryptor.

The security services provided by TrustCrypt are AES, SHA, RSA and DRNG through the RS232 serial port.

Customized application can be downloaded into the TrustCrypt if needed. The customized application to be downloaded will be signed by approved authority using RSA.

Key Features and Benefits

- FIPS 140-2, Level 3 certified
- AES, SHA, RSA and DRNG security services
- Security services easily accessed after authentication through RS232 serial port
- Can be used as cryptographic core for other security products
- Easily customizable by downloading signed customized application by approved authority



SPECIFICATIONS

General	<ul style="list-style-type: none"> • FIPS 140-2 level 3 certified • Cryptographic variables backup by external battery
Cryptography / Authentication	<ul style="list-style-type: none"> • AES 128, 192, 256 in ECB, CBC, OFB, CFB128 mode • SHA-256 and SHA-512 • RSA 1024 and 2048 using PKCS v1.5 • DRNG with AES-128 (ANSI X9.31)
Security	<ul style="list-style-type: none"> • Encased in a hard opaque commercial grade epoxy • Active zeroization of cryptographic data • KEK Publishing Authority for downloading Key • Application Publishing Authority for downloading customized application
Diagnostics	<ul style="list-style-type: none"> • Automatic Power-up self-tests
Interface	<ul style="list-style-type: none"> • RS232 UART • GPIO pins
Operating Environment	<ul style="list-style-type: none"> • Operating temperature: 0°C to +50°C • Relative Humidity: 0 to 90% • Meets FCC Part 15, Class B EMI/RFI requirements
Electrical & Mechanical	<ul style="list-style-type: none"> • Mains: 110/230 VAC 50/60 Hz • Dimension: 85W x 10H x 55Dmm