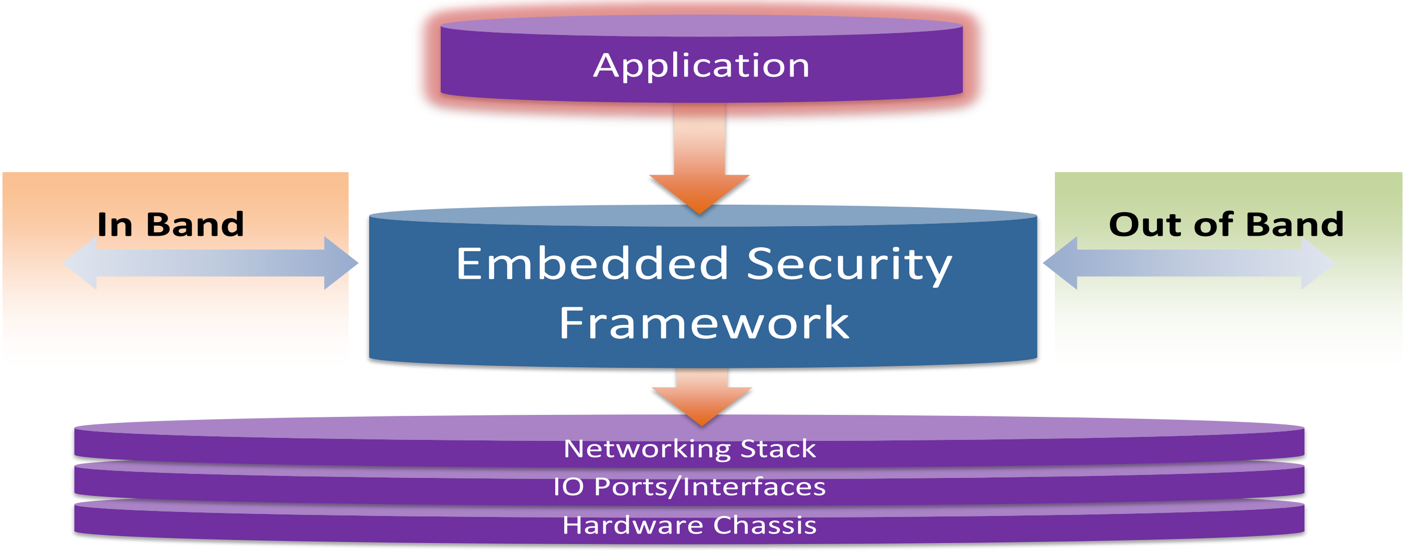
Embedded Security Framework

TELEGRID

The Embedded Security Framework (ESF) developed by TELEGRID is a structured collection of encryption and authentication modules designed to accelerate the design and development of embedded systems. It is based on TELEGRID's 30+ years of design, development and production of embedded systems in the field of voice and data encryption, secure unified communications and management of networked encryptors.

The framework was developed in line with DISA's Secure Technical Implementation Guides (STIGs). It includes a FIPS 140-2 compliant encryption engine as well as DoD approved mutual authentication methods (i.e., PKI). Additionally it includes integration into centralized authentication services including RADIUS and LDAPS as well as support for Out of Band management via SNMPv3.

The ESF helps Government Engineers design STIG compliant embedded systems quickly. The Framework includes all relevant documentation (e.g., FIPS 140-2 certificate, STIG questionnaire, etc.) to speed the certification process. By incorporating security early in the development cycle product designers can eliminate late-stage redesigns thereby reducing cost and development time.



Features

- Modular security and authentication to speed design and development of embedded systems

- FIPS 140-2 Compliant encryption engine
  - FIPS validated algorithms and modules
  - Pre-compiled FIPS 140-2 compliant applications (Apache, OpenSSH, OpenVPN, etc.)

- Public Key Infrastructure (PKI) Support
  - CAC/PIV credential-enabling
  - LDAP Integration with Active Directory
  - PKI certificates for mutual authentication
  - Certificate loading and installation for upload into a DoD Certificate Authority (CA)
  - Configuration of a root of trust/ trust anchor to support chained certificate validation
  - Revocation checking - Online Certificate Status Protocol (OCSP) or Certificate Revocation Lists (CRL)

- Centralized Authorization protocol support
  - System access validation via RADIUS, TACACS+ and Diameter

- Developed in line with DISA Secure Technical Implementation Guides (STIGs)
  - Reduces late-stage redesigns for non-STIG compliant encryption and authentication
  - Includes relevant documentation to speed certification

Embedded Security Framework Development Board

The Embedded Security Framework is available on an industrial grade single board computer for rapid prototyping. The high powered quad core microprocessor has 2GB RAM and 4GB Flash. It includes wide area network connectivity through multiple high speed interfaces (PCIe, SATA, Gigabit Ethernet) and up to 135 GPIOs for integration into any system. It is available as a standalone board or as a development kit with multiple inputs/ outputs for prototyping.

Capabilities

Cryptography	
FIPS 140-2 Level 1 Compliance	Yes
Public / private key pair generation / certificate signing request	Yes
Symmetric Key Cryptography	Yes
Hashing	Yes
Random Number Generation	Yes
Protocols	
HTTPS	Yes
IPSec	Yes
TLS (version 1.1 minimum per NIST SP 800-52)	Yes
SSH (v2)	Yes
NTPv3 / v4 compliant	Yes
SNMPv3 / v2c	Yes
Syslog	Yes
Public Key Infrastructure (PKI)	
Supports Multiple Public Key Infrastructures	Yes
Certificate revocation checking (OCSP and CRL)	Yes
Supports PKI-based Two Factor authentication	Yes
Authentication, Authorization, Accounting (AAA)	
Supports Centralization Authentication and Authorization	Yes
802.1x Support	Yes
Auditing	
Audit log / trail	Yes