CyPRSS

Root of Trust (RoT)
Lattice-based Network

Extending embedded RoT to the network to provide enhanced protection for the entire network stack

Cyber Secure Processing for Resilient & Survivable Systems (CyPRSS) extends the embedded Root of Trust (RoT) to the network through lattice-based access. This is done by ensuring trust currency from the hardware anchors crosses the network stack to reach mission devices that may not be hardware RoT enabled.

CyPRSS extends the RoT architecture by serving as middleware to extend the trust from power on and secure boot capabilities, and securing applications and network connectivity beyond standard network operations and methods.

CyPRSS provides a portable, scalable, user-friendly, and effective cyber resilience architecture and software development kit for use with any Trusted Computer Group (TCG) Trusted Platform Module (TPM) version 2.0 hardware. This can be done with or without a customized RoT secure processor/trust anchor or the use of COTS RoT solutions that enable encryption keys specific to a host system.

CyPRSS ensures hardware, software, and network authentication form an encryption-based "Root of Trust" with specific key design features that include:

- Trusted Servers with bi-directional verification of trusted servers
- Lattice-based network access configuration for servers and nodes (extending trust to mission devices)
- Heartbeat 'verification' capability that is configurable
- Generalized trust management using:
  - TPM 2.0 to standardize use of custom or COTS secure hardware
  - Non-TPM 2.0 standardization for customized solutions
  - Standardized TCP Sockets communications, messaging
  - Standardized DDS common interfaces
  - Integrity measurements and trust auditing through:
    - TPM 2.0 TCG Trusted Attestation Protocol (TAP) Information Model
    - Standardized trusted secure heartbeat

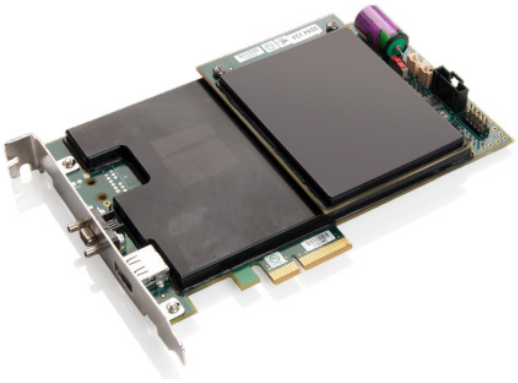
CyPRSS provides a plug and play generic middleware solution for reusing known Root of Trust (RoT) components (e.g., customized GOTS secure processors, COTS, and virtual) that extends an embedded RoT, or trust anchor, to the network through trust currency in a lattice-based access design. Trust anchors extend the trust from hardware through the network and mission system's devices at a lower cost using COTS-based designs to provide secure, trusted weapon system authentication constructs.

CyPRSS offers the capability to address weapon system authentication outside the standard operating environments, using a trust anchor to form a trust currency.

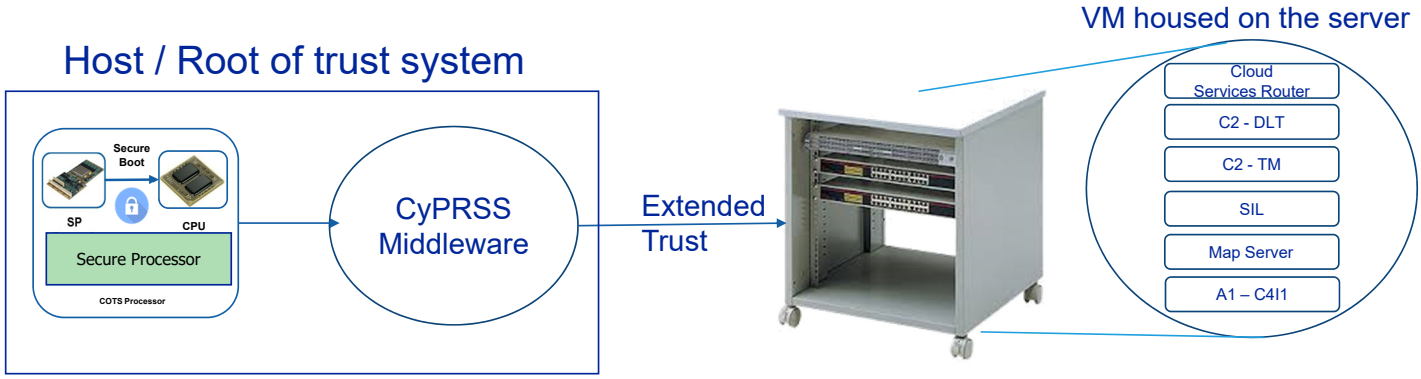
CyPRSS on a Card (COC) is designed to provide a middleware application resident on a secure hardware platform such as:

- Thales ProtectServer PCIe HSM 2
- FIPS 140-2 Level 3 validated
- Tamper-protected environment
- Dimensions: Full Height, Half Length 4.16" x 6.6"
- (106.7mm x 167.65mm)
- Temperature: operating 0°C – 50°C
- CyPRSS Secure Linux Core

Through CyPRSS, Northrop Grumman has developed a method of securely booting from a trusted device, so that an adversary is not able to exploit this critical time and tamper with mission critical systems. The CyPRSS team enables a secure environment from a RoT and continuous attestation of the system security (i.e., start secure, stay secure). Northrop Grumman has identified the complexity and variety of needs that contribute to enabling these capabilities and, with that focus in mind, developed the CyPRSS application to govern bringing these systems online securely.



CyPRSS is available in virtual or on-card options



CyPRSS extends RoT across networked systems

Exemplar Weapon System

For more information, please contact:
Northrop Grumman Mission Systems
Rusty Toth
Phone: 703-949-2335
roger.toth@ngc.com

northropgrumman.com

NORTHROP GRUMMAN