

Trusted Embedded Environment (TEE)

A General Dynamics High Assurance Open Scalable Technology (G.H.O.S.T.)



An Assured Edge for Your Network

Certifiable multilevel capabilities extended from a secure separation kernel through General Dynamics' multilevel systems expertise

Information across multiple domains on a single platform

Virtualization approach save costs

General Dynamics High Assurance Open Scalable Technology (G.H.O.S.T.)

General Dynamics High Assurance Open Scalable Technology (G.H.O.S.T.) is a suite of high-assurance, trusted technologies that deliver multi-domain and cross-domain solutions, policy-based management technology for managing the GIG enterprise, and comprehensive security architectures with integrated IA solutions for accreditation of high assurance systems.



The G.H.O.S.T. suite represents a quantum leap in the way military and government security levels are accessed and the speed with which government organizations can operate and communicate around the world. G.H.O.S.T. reduces the need for multiple computers to access different security levels which results in overall cost reductions in both hardware and network support while increasing system-wide mobility.

Trusted Embedded Environment (TEE)

A General Dynamics High Assurance Open Scalable Technology, the Trusted Embedded Environment (TEE) provides capabilities that enable processing and interfacing with information at multiple security levels. The TEE Technology shelf provides capabilities for use in tactical multilevel situations that leverages the underlying Separation Kernel/Hypervisor for high-assurance systems. TEE is an enabling technology, providing interfaces for developing applications in a MILS environment. TEE is targeted towards tactical embedded environments and is scalable to workstation and server environments. TEE builds upon the jointly developed LynxWorks LynxSecure core Separation Kernel/Hypervisor for trusted display, cross domain, and other secure multi-level scenarios. TEE provides cross-domain solutions for both information access and transfer scenarios.

TEE enables a robust environment within which entire operating systems, such as Microsoft® Windows®, Linux®, and LynxOS-SE®, run in different security domains such as Top Secret, Secret and Unclassified, simultaneously, with no compromise of security, reliability or data. Legacy applications run unmodified on supported guest operating systems reducing total cost of ownership. TEE also supports cross-domain applications. High-robustness allows simultaneous hosting of non-adjacent security domains (e.g., U and TS).

TEE supports open standards, and offers runtime POSIX that is designed to allow development of high-robustness trusted applications. TEE is compliant with the U.S. Government Protection Profile for Separation Kernels in Environments Requiring High Robustness (SKPP). It leverages commercial-off-the-shelf x86 virtualization technology from Intel. Its extremely small code size eases evaluation and certifiability, and it supports Safety-Critical & Real-Time (certifiable to RTCA DO-178B, ARINC-653) applications.

Trusted Embedded Environment (TEE)

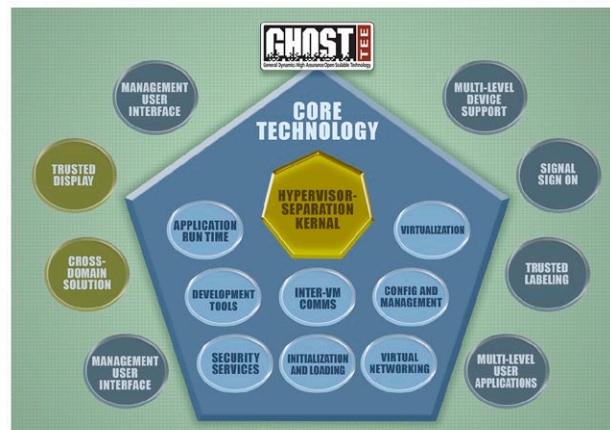
TEE's advanced security features are provided both by hardware assistance using Intel® Virtualization Technology (VT-x and VT-d) and by high-assurance separation kernel software from General Dynamics. TEE conforms to the Multiple Independent Levels of Security (MILS) architecture, partitioning system data and resources and controlling information flow between partitions.

Benefits

- Maximizes agility and flexibility; improved interoperability, security, configurability, scalability and information sharing
- Supports multiple heterogeneous operating system environments on a single hardware platform
- Supports unmodified legacy applications on multiple operating systems
- Implements trusted hardware partitioning for multilevel scenarios
- Support for open standards
- Reduces computing and infrastructure costs
- Eliminates "periods processing," improves operational workload and reduces errors, since multiple security domains are simultaneously available
- Enables cross-domain services without the need for custom or individual hardware
- Portable to multiple processor architectures with anticipated minimal impact on evaluation
- Utilization of processor specific optimizations
- Flexible architecture supports wide range of customizations to meet varying needs

Features

- Builds upon the jointly developed LynxWorks LynxSecure core Separation Kernel technology for trusted display, cross domain transfers, and other secure multilevel scenarios



- DO-178B Level A certifiable
- Trusted time and space separation
- Hard real-time, deterministic scheduling supports RTOS
- Hypervisor and virtualization technology
- Highly scalable technology
- Runs on x86 64-bit processor
- Able to host both 32- and 64-bit guest operating systems and applications
- Supports para-virtualized and fully virtualized operation systems
- Supports Symmetric Multiprocessing (SMP) operating systems (future)
- Supports multi-core
- Flexible scheduling policy
- 100 percent binary compatible Linux- or POSIX-based software applications
- Supports cross-domain applications including the G.H.O.S.T. Tactical Cross-Domain Guard
- Strictly controlled information flows between virtual machines
- Separate memory spaces (strong separation between virtual machines)
- Designed to comply with U.S. Government Protection Profile for Separation Kernels in Environments Requiring High Robustness
- Failures and compromises are isolated to a single virtual machine

- Secure boot
- Does not require custom hardware or BIOS

Guest Operating Systems

- Linux®
- LynxOS-SE®
- Red Hat Enterprise Linux® 4 & 5
- Microsoft® Windows® XP
- Solaris (future)

Technology Shelf

- Extends core capabilities to provide multilevel functions: display, management, partitioning, security
- Multilevel display toolbar, user access control, startup, shutdown, health status, and auditing
- Multilevel capability integration expertise

Operational Environments

- Designed for simultaneous Top Secret/Secret/Unclassified (DCID 6/3 PL-5)
- Intel-based hardware platforms
 - Intel 945, 965, ICH9M
- General Dynamics hardware platforms
 - PC3030, PC3034, SNP2 3U single board computers
 - SD7310 Smart Display

GENERAL DYNAMICS

C4 Systems

8220 East Roosevelt Street, M/D R7229 • Scottsdale, Arizona 85257 • Website: www.gdc4s.com/tee
General Dynamics contact: Phone: 480-441-5448 • Toll-free: 866-400-0195 • Email: IASystems@gdc4s.com

© 2010 General Dynamics. All rights reserved. All trademarks indicated as such herein are trademarks of General Dynamics. All other product and service names are the property of their respective owners. ® Reg. U.S. Pat. and Tm. Off. General Dynamics reserves the right to make changes in its products and specifications at any time and without notice.