SIERRAWARE

SIERRATEE FOR MIPS OMNISHIELD™

Introduction

SierraTEE for MIPS OmniShield™ is a Global Platform compliant Trusted Execution Environment (TEE) designed for devices based on Imagination Technologies' MIPS OmniShield-ready CPUs. It provides a secure area within a connected device that ensures sensitive data is stored, processed and protected in an isolated, trusted environment—enabling end-to-end security by offering isolated, safe execution of authorized security software.

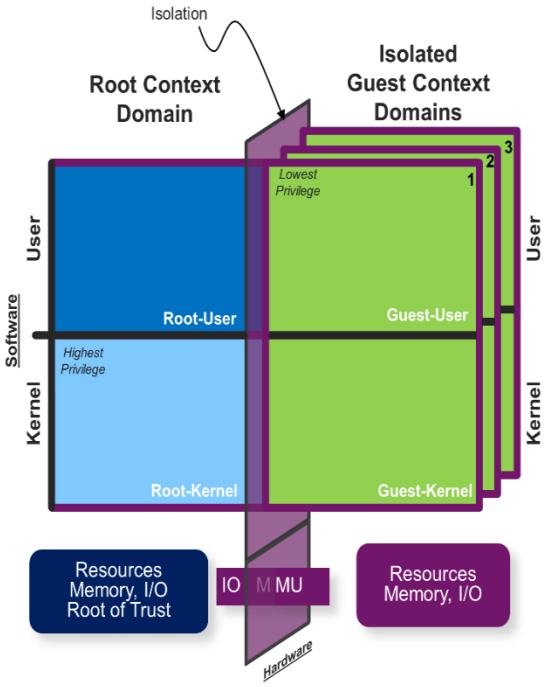
SierraTEE provides an easy-to-implement security solution for MIPS CPUs. It is implemented through Imagination's OmniShield technology, which leverages hardware virtualization in the MIPS CPU to enable the creation of multiple domains. SierraTEE uses OmniShield virtualization technology to completely protect the secure kernel and associated peripherals from code running in the rich environment. This means that even if an attacker manages to obtain full supervisor privileges in the Rich OS it cannot gain access to the secure domain.

In a system with multiple domains, SierraVisor enables isolation of multiple concurrent guest systems. The combination of the SierraVisor and Sierraware TEE allows full operation of the TEE and rich environments isolated in each domain environment.

What is OmniShield?

OmniShield scales beyond a binary approach to create multiple secure domains in a CPU and GPU, where each secure/non-secure application can operate independently in its own separate domain.

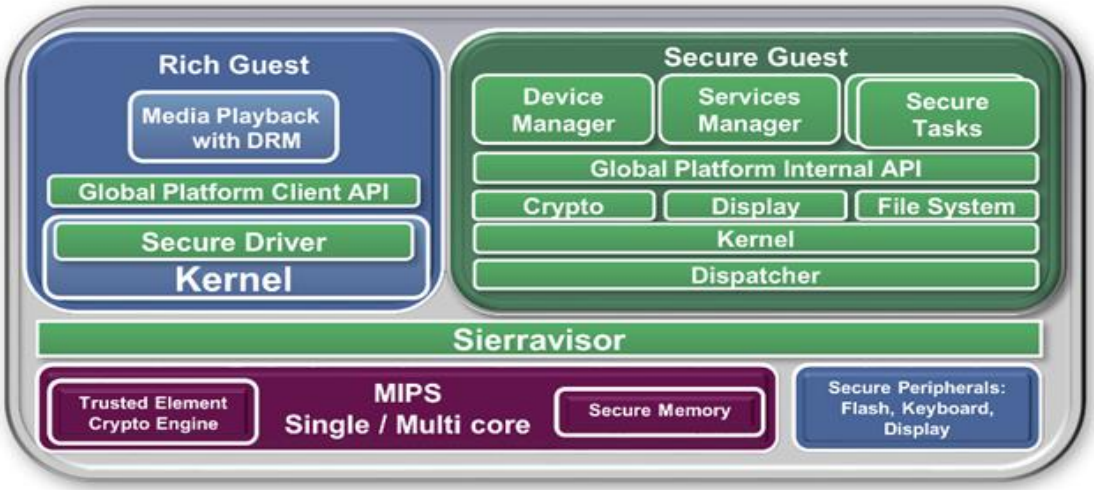
The use of hardware virtualization ensures security through separation, enforcing a clean-room environment operation of applications while preventing cross-contamination and leaks. In addition, this technology enables the separation and protection of critical assets such as device communication interfaces (and software stacks), storage and other resources into their own address spaces, and ensures there is no access from/to any other applications' address spaces. Each of these separate memory spaces is known as a 'domain'. Each system function can only use its own domain and normally can't access the domains used by other functions. By having multiple domains, each single function is isolated from other functions and the rest of the system.



The OmniShield architecture allows construction of up to 255 domains, but most implementations generally require a lower number of domains; typically two to eight domains. Access to memory spaces which are shared among multiple domains is programmatically controlled by privileged Root-Kernel.

With its unique architecture and methodology, OmniShield offers numerous benefits:

- CPU consolidation
- Isolate critical software
- Secure updates
- Reduction in QA, testing and certification
- Accelerated time-to-market

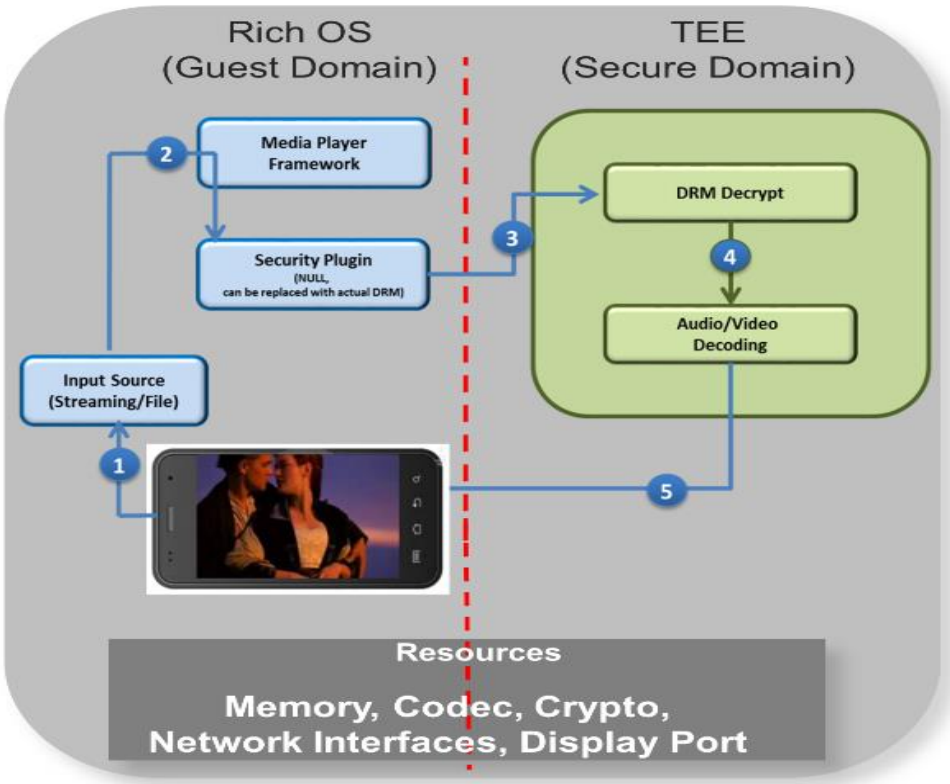


Global Platform Compliant TEE

SierraTEE for MIPS is a comprehensive implementation of MIPS hardware backed virtualization as well as Global Platform System and Inter Process Communication (IPC) APIs.

Sierraware TEE offers a wide range of capabilities and applications, providing a simple, affordable way to integrate rich platforms like FFmpeg, OpenSSL, MiniDLNA, and others. In addition to offering a full suite of Global Platform APIs, it offers POSIX APIs for easy integration of legacy applications like DRM with minimal changes. POSIX also allows for building devices with very small footprint ideal for applications like IoT and set-top boxes. The secure kernel is optimized for size and performance while maintaining POSIX compliance. SierraTEE offers a wide range of APIs and features. The table below describes some of the salient features offered.

Item	Description
1	Software Crypto Library for most of major protocols like RSA, AES, PKI
2	POSIX Application interface for Task creation, File system, Timers etc.
3	Secure Element API. Integrated with several popular SE devices
4	Global Platform 2.0 API
5	Global Platform Test Platform. Allows all OEMs to generate Test report with a one click report generator. Allowing them to save in certification costs.
6	Secure Sockets



Secure Video Datapath

- Having a secure video datapath mandates that both compressed and un-encrypted content must be kept out of the Guest memory space.

- A single video rendering path executed on the TEE must serve multiple Guest operating systems.
- Physical memory translation between Guest and TEE must be handled by an integrated solution.
- Arbitration of resources is another important factor.
- The ability to share hardware codecs and devices like speakers between multiple guests in a secure way is critical.

OmniShield
by Imagination

OmniShield enables companies for the first time to implement a scalable, heterogeneous multi-domain security environment. OmniShield is scalable to address the next generation of devices: able to support multi-threaded, multi-core, multi-cluster designs and heterogeneous architectures. It can also support multiple isolated trusted applications by enabling the creation of multiple secure domains. OmniShield also addresses the scalability that heterogeneous architectures require by protecting all of the processors in an SoC – including the CPU, GPU and others. As security is no longer a CPU bound problem,

Imagination is in a strong position to deploy trust more effectively than others by building protection into our complete portfolio of IP for SoCs.

About Sierraware

Sierraware is a leading provider of virtualization and security solutions that change the way applications are accessed and data is secured. Sierraware's virtual mobile infrastructure (VMI) software empowers developers to support all mobile platforms with a single app and to protect data and monitor user activity. SierraVisor Hypervisor and SierraTEE Trusted Execution Environment for ARM® TrustZone® deliver embedded virtualization platforms for ARM based architectures.

1250 Oakmead Parkway
Suite 210
Sunnyvale, CA 94085
United States
Phone: +1 408-337-6400
Email: info@sierraware.com