Intel® Trust Domain Extensions (Intel® TDX)

Published: 08/11/2020

Last Updated: 03/08/2023

By Jiewen Yao

Overview

Intel® Trust Domain Extensions (Intel® TDX) is introducing new, architectural elements to help deploy hardware-isolated, virtual machines (VMs) called trust domains (TDs). Intel TDX is designed to isolate VMs from the virtual-machine manager (VMM)/hypervisor and any other non-TD software on the platform to protect TDs from a broad range of software. These hardware-isolated TDs include:

- Secure-Arbitration Mode (SEAM) – a new mode of the CPU designed to host an Intel-provided, digitally-signed, security-services module called the Intel TDX module.
- Shared bit in GPA to help allow TD to access shared memory.
- Secure EPT to help translate private GPA to provide address-translation integrity and to prevent TD-code fetches from shared memory. Encryption and integrity protection of private-memory access using a TD-private key is the goal.
- Physical-address-metadata table (PAMT) to help track page allocation, page initialization, and TLB consistency.
- Multi-key, total-memory-encryption (MKTME) engine designed to provide memory encryption using AES-128- XTS and integrity using 28-bit MAC and a TD-ownership bit.
- Remote attestation designed to provide evidence of TD executing on a genuine, Intel TDX system and its TCB version.

Intel TDX White Papers and Specifications – Common

Document	Description
Intel® Trust Domain Extensions (Intel® TDX)	An introductory overview of the Intel TDX technology.
Intel® CPU Architectural Extensions Specification	A specification of Intel CPU architectural support for Intel TDX.
Intel® TDX Loader Interface Specification	A specification of how a VMM loads the Intel TDX Module on a platform.
Intel® TDX Virtual Firmware Design Guide	A design guide on how to design and implement a virtual firmware for a trust

Intel TDX 1.0 White Papers and Specifications

Document	Description	Date
Intel® TDX Module 1.0 Specification	Architecture and Application Binary Interface (ABI) Specification of the Intel TDX Module.	February 2023
Intel® TDX Guest-Hypervisor Communication Interface	Specification of the software interface between the Guest OS (Tenant) and the VMM required for enabling Intel® TDX 1.0	December 2022

Intel TDX 1.5 White Papers and Specifications

Intel® TDX Version 1.5 extends TDX to introduce Live Migration and TD Partitioning for TD VMs and related support for Service TDs.

Document	Description	Date
Intel® TDX Module v1.5 Base Architecture Specification	Overview and base architecture specification of the Intel TDX Module version 1.5	March 2023
Intel® TDX Module v1.5 TD Migration Architecture Specification	Overview and architecture specification of the TD Migration feature of the Intel TDX Module version 1.5	March 2023

Document	Description	Date
Intel® TDX Module v1.5 TD Partitioning Architecture Specification	Overview and Architecture Specification for TD partitioning of the TDX Module version 1.5	March 2023
Intel® TDX Module v1.5 ABI Specification	Application Binary Interface (ABI) specification of the Intel TDX Module version 1.5	March 2023
Intel® TDX Module Incompatibilities between v1.0 and v1.5	Description of the incompatibilities between TDX 1.0 and TDX 1.4/1.5 that may impact the host VMM and/or guest TDs	March 2023
Intel® TDX Guest-Hypervisor Communication Interface v1.5	Specification of the software interface between the Guest OS (Tenant and Service TD VMs) and the VMM required for enabling Intel TDX version 1.5	July 2022
Intel® TDX Migration TD Design Guide	A design guide on how to design and implement a Migration TD for TDX 1.5 Live migration.	October 2021

Intel TDX Connect Whitepapers and Specifications

Intel® TDX Version 2.0 extends TDX to support Trusted Execution Environment for device I/O (TEE-IO).

Document	Description	Date
Intel® TDX Connect TEE-IO Device Guide	An introductory overview on how to build TEE-IO device for confidential computing compliant with PCIe TDISP 1.0 and compatible with Intel® TDX Connect	February 2023
Device Attestation Model in Confidential Computing Environment	An introductory overview of the device attestation in confidential computing.	September 2022
Software Enabling for Intel® TDX in Support of TEE-IO	White paper to introduce how to enable software for Intel TDX with TEE-IO device.	September 2022

Intel TDX Source Code

Source Code	Version	Description	Date
Intel® TDX Loader	TDX 1.0	TDX Loader source code including instructions for reproducible build.	August 2022
Intel® TDX Module	TDX 1.0	TDX Module source code including instructions for reproducible build.	August 2022

Intel TDX Security Guidance

Page	Date
Intel® TDX Guidance for Developers	March 2023
Intel® TDX Guest Kernel Hardening Documentation	March 2023

Product and Performance Information

[1] Performance varies by use, configuration and other factors. Learn more at www.Intel.com/PerformanceIndex .

Investors

Careers

Corporate Responsibility

Diversity & Inclusion

Public Policy

Terms of Use

*Trademarks

Cookies

Privacy

Supply Chain Transparency

Site Map

Recycling