Intel TDX Overview
Trust Boundary of Confidential Computing (CC)

Without Confidential Computing

- Cloud Stack & Admins
- BIOS & Firmware
- Host OS & Hypervisor
- VM Guest Admin
- Guest OS
- Applications
- Confidential Data

VM Isolation with Intel® TDX

- Cloud Stack & Admins
- BIOS & Firmware
- Host OS & Hypervisor
- VM Guest Admin
- Guest OS
- Applications
- Confidential Data

App Isolation with Intel® SGX

- Cloud Stack & Admins
- BIOS & Firmware
- Host OS & Hypervisor
- VM Guest Admin
- Guest OS
- Apps
- Enclave
- Confidential Data
Intel Trust Domain Extensions (Intel TDX) – Overview

- **Host VMM (TDX-Enlightened)**
  - Isolation provided by Host VMM
  - Legacy VM
    - Applications
    - OS
  - Host OS
    - Guest-Side API

- **Intel TDX Module**
  - Intel TDX Guest-Side API
  - Trust Domain
    - Unmodified Applications
    - TDX-Enlightened OS
  - Intel TDX Host-Side API

- **Memory**
  - Plaintext
  - Encrypted with Key 1
  - Encrypted with Key 2

- **Rest of Platform (Cores, Caches, Devices, etc.)**
## Intel TDX Linux Enabling

### Attestation Services
- TD Verification Service
- Key Broker Service
- Provisioning Certificate Enclave
- TD Quote Verification Service
- PCCS

### Attestation Primitive
- TD Quoting Enclave
- Provisioning Certificate Enclave
- TD Quote Driver in TD Guest
- Attestation Agent in TD Guest

### Orchestration
- LibVirt

### VMM/Containers
- KVM
- QEMU
- CoCo

### OS
- Cent OS
- Ubuntu
- SUSE

### Kernel
- Host Linux Enabling
- TD Linux Guest Enabling

### BIOS/FW
- SEAMLR
- TDX Module
- vBIOS (TDVF) in VM

### Silicon
- TDX ISA
- TDX Live Migration

---

**Open Source**

**Non-Open Source**

**Reference Implementation**

---

Intel Security Center of Excellence
Intel TDX Availability

Intel TDX became available on select 4\textsuperscript{th} Gen Intel Xeon Scalable instances through four leading cloud providers.

Previews began as early as Q1’23; Check with your provider for their availability dates.

Intel TDX became generally available with 5\textsuperscript{th} Gen Intel Xeon Scalable processors (code-named Emerald Rapids).
Intel TDX Details
<table>
<thead>
<tr>
<th>Feature</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>CPU-State Confidentiality</strong></td>
<td>TD state managed in CPU-protected memory and invisible to non-TD system SW</td>
</tr>
<tr>
<td><strong>Memory Confidentiality and Integrity</strong></td>
<td>Using access-control and per-TD private key to mitigate VMM attacks from modifying or observing tenant’s memory, whether in cache or DDR</td>
</tr>
<tr>
<td><strong>Key Management and Key-ID partitioning</strong></td>
<td>Ability to create, retrieve, use, and manage encryption keys along the lifetime of a TD. Coexist with TMEi-MK usage by host SW.</td>
</tr>
<tr>
<td><strong>Remote Attestation</strong></td>
<td>Authenticate platform and TD image at TD launch time. Leveraging SGX attestation.</td>
</tr>
<tr>
<td><strong>I/O Compatibility</strong></td>
<td>Synthetic and Direct I/O support to shared memory. Support for MMIO emulation.</td>
</tr>
<tr>
<td><strong>Platform Analysis</strong></td>
<td>SW debug/tuning without loss of confidentiality.</td>
</tr>
<tr>
<td><strong>Memory management</strong></td>
<td>Secure EPT memory mgmt. for private TD memory – to address EPT remap attacks</td>
</tr>
</tbody>
</table>
Intel TDX Module + SEAM

- Intel TDX Module
  - Intel-provided and Intel-signed
  - SEAM Loader (SEAMLDR) verifies Intel TDX Module and loads it into SEAMRR
  - SEAMRR protected with AES-XTS

- Secure Arbitration Mode (SEAM)
  - Intel TDX Module operated in SEAM VMX-root mode
  - ISA instructions added to enable host & guest interactions: SEAMCALL, SEAMRET, TDCALL, SEAMOPS
  - Mode-restricts use of certain ISA instructions
TDX Remote Attestation

- TD proves to a third/relying party that
  - the booted TD image exactly as expected (MRTD)
  - the measurements created/extended during runtime are as expected (RTMRs)
  - the TD is executed on an Intel TDX-enabled platform
  - the Intel TDX-enabled platform is fully up to date

- Third/relying party can use this proof to decide if TD is trusted
TDX Remote Attestation

- Process:

  - TD Quote (Attestation Key Signed)
  - Attestation Key Cert. (PCK Signed)
  - PCK Certificate (Intel Signed)

- TDX leverages Intel SGX attestation:
  - One set of PCK certificates, distribution, caching services to support SGX & TDX
  - Requires SGX be enabled in host for TDX attestation
## Attestation Verification Options

<table>
<thead>
<tr>
<th>Attestation Verification Options</th>
<th>Cloud Provider’s Attestation Service</th>
<th>Application Vendor’s Attestation Service</th>
<th>Independent Trust Service (e.g., Intel® Trust Authority)</th>
<th>Build-Your-Own Service with Intel Library</th>
</tr>
</thead>
<tbody>
<tr>
<td>Separation of responsibilities between verifier and infrastructure provider</td>
<td>No</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>Consistency across Intel SGX and Intel TDX</td>
<td>Yes, if both Intel SGX and TDX offered</td>
<td>Yes, if both Intel SGX and TDX supported</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>Consistent service across on-prem, hybrid, multi-cloud, and edge deployments</td>
<td>No</td>
<td>Possible, but limited to specific application</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>Development effort</td>
<td>Low</td>
<td>Low</td>
<td>Low</td>
<td>Medium</td>
</tr>
</tbody>
</table>
Upcoming Features
TD Migration

Source Platform

- Migration TD
- Migrated TD
- TDX Metadata API
- Session Control
- Session Control, Keys Exchange
- Session Control, TD Non-Memory State, TD Private Memory

Destination Platform

- Migration TD
- Migrated TD
- TDX Metadata API
- TDX Import API
- TDX Export API
- Session Control
- Session Control, Keys Exchange
- Host VMM
Intel TDX Connect

Goal: Enable heterogenous confidential computing with secure, efficient, and low-overhead data movement to/from devices

### TDX 1.0/1.5

- No devices trusted by any TD
- Devices cannot access TD private memory
- Overheads for (secure) data movement

### Intel TDX Connect

- ✓ TD trust can be extended to trusted
- ✓ Trusted devices can access TD private memory
- ✓ Efficient, low-overhead data movement (PCIe, CXL)

---

- Encrypt & copy-out
- Decrypt & copy-in

- Encrypt & copy-out
- Decrypt & copy-in
# TDX White Papers and Specifications

Browse Intel TDX Documentation
Find documentation and explore resources designed for easy access and hands-on learning.

Jump to Architecture | Source Code | Security Guidance

## Intel TDX Architecture

### Common Intel TDX White Papers and Specifications

<table>
<thead>
<tr>
<th>Document</th>
<th>Description</th>
<th>Last Updated</th>
</tr>
</thead>
<tbody>
<tr>
<td>Intel® Trust Domain Extensions (Intel® TDX)</td>
<td>An overview of the Intel TDX technology</td>
<td>February 2023</td>
</tr>
<tr>
<td>Intel CPU Architectural Extensions Specification</td>
<td>A specification of Intel CPU architectural support for Intel TDX</td>
<td>May 2021</td>
</tr>
<tr>
<td>Intel TDX Loader Interface Specification</td>
<td>A specification of how a virtual machine manager (VMM) loads the Intel TDX Module on a platform</td>
<td>March 2022</td>
</tr>
<tr>
<td>Intel TDX Virtual Firmware Design Guide</td>
<td>A guide on how to design and implement a virtual firmware for a trust domain</td>
<td>December 2022</td>
</tr>
</tbody>
</table>

## Intel TDX 1.0

<table>
<thead>
<tr>
<th>Document</th>
<th>Description</th>
<th>Last Updated</th>
</tr>
</thead>
<tbody>
<tr>
<td>Intel TDX Module 1.0 Specification</td>
<td>Architecture and Application binary interface (ABI) specification of the Intel TDX module</td>
<td>February 2023</td>
</tr>
<tr>
<td>Intel TDX Guest- Hypervisor Communication Interface</td>
<td>Specification of the software interface between the guest operating system (kernel) and the VMM required to enable Intel TDX 1.0</td>
<td>March 2023</td>
</tr>
</tbody>
</table>

Legal Disclaimer

Intel® technologies may require enabled hardware, software, or service activation.

No product or component can be absolutely secure.

Your costs and results may vary.

©Intel Corporation. Intel, the Intel logo, and other Intel marks are trademarks of Intel Corporation or its subsidiaries. Other names and brands may be claimed as the property of others.