TCB Composition

The Trusted Computing Base (TCB) includes all hardware and software components that must be trusted for security. TCB components can be:

Immutable Components

- Cannot be changed post-manufacture
- Typically implemented in hardware
- Examples: RTM, hardware-based isolation

Mutable Components

- Can be updated during platform lifetime
- Usually implemented in software
- Updates reflected in attestation reports
- Examples: measurement code, attestation

Most TEEs use a mix of mutable and immutable components in their TCB.

TCB Components by Function

Verifiable Launch

RTM is immutable in all TEEs, while measurement and attestation are typically mutable

Run-time Isolation

Most TEEs use mutable software TCB for CPU context switching and memory isolation

Trusted IO

Most TEEs with trusted IO rely on mutable software TCB

Secure Storage

Implemented either through TPM, software TCB, or hardware instructions

The ability to update TCB components is crucial for addressing vulnerabilities without product recalls.

TCB Size Considerations

TCB size is often measured in lines of code (LoC) for mutable components:

0-1K

Minimal TCBs

Academic proposals like Flicker, Sanctum, and Komodo focus on minimal TCB size

2-10K

Moderate TCBs

RISC-V TEEs like Keystone and Penglai have moderate TCB sizes

50K+

Commercial TCBs

ARM TrustZone and IBM PEF have larger TCBs with more features

TCB size alone is not a good metric for comparing TEEs, as it doesn't account for feature differences, implementation quality, or verification efforts.

Comparative Analysis: TCB Size

75K

IBM PEF software monitor size (lines of code)

50K

ARM TrustZone OP-TEE implementation (lines of code)

16.5K

Keystone secure boot code (lines of code)

5K

Sanctum security monitor (lines of code)

0.8K

Komodo security monitor (lines of code)

TCB size varies widely, with commercial implementations generally having larger codebases than academic proposals. However, TCB size alone is not a good metric for security or functionality.

Comparative Analysis: RTM and Attestation

Name	ISA	RTM	Local Attestation	Remote Attestation
Intel SGX	x86	DRTM	✓	✓
Intel TDX	x86	DRTM	✓	✓
AMD SEV-SNP	x86	SRTM	✓	✓
ARM TZ	ARM	SRTM	-	✓
ARM Realms	ARM	SRTM	-	✓
Keystone	RISC-V	SRTM	-	✓

Most TEEs use SRTM, with only Intel solutions using DRTM. Remote attestation is universally supported, while local attestation is less common.

Comparative Analysis: CPU Isolation

Name	Isolation Strategy	Enclave Type	Software TCB Level
Intel SGX	Temporal-Logical	Application	-
Intel TDX	Temporal-Logical	VM	PL1
AMD SEV-SNP	Temporal-Logical	VM	Co-processor
ARM TZ	Temporal-Logical	App/VM	PL0+(PL1/2)
ARM CCA	Temporal-Logical	VM	PL0+(PL1)
Sanctum	Temporal-Logical	Application	PL0

All TEEs use temporal-logical isolation for CPU state. Enclaves run as either applications (PL3) or VMs (PL2), while software TCB components run at higher privilege levels.

Comparative Analysis: Memory Isolation

Name	Software Adversaries	Physical Adversary	Access Control
Intel SGX	Spatio-temporal Logical	Cryptographic	Page Tables
Intel TDX	Spatio-temporal Logical	Cryptographic	Page Tables
AMD SEV-SNP	Spatio-temporal Cryptographic	Cryptographic	Page Tables
ARM TZ	Spatio-temporal Logical	Cryptographic (optional)	Page Tables
Keystone	Spatio-temporal Logical	-	MPU
AEGIS	Spatio-temporal Cryptographic	Cryptographic	Extra Metadata

Memory isolation strategies vary widely, with different approaches for software vs. physical adversaries. Commercial TEEs tend to use page tables, while academic TEEs often use MPUs.

Comparative Analysis: Trusted IO and Secure Storage

Name	Trusted IO	Secure Storage
Intel SGX	-	Hardware instructions
Intel TDX	-	-
AMD SEV-SNP	-	Primitives only
ARM TZ	TrustZone Protection Controller	Software TCB
ARM CCA	Realm Management Extension	-
CURE	IO filters	-
Keystone	-	Software TCB

Trusted IO and secure storage are less universally supported than other security goals. Only about a third of TEEs explicitly discuss sealing support.

Comparative Analysis: TCB Composition

Name	RTM	Measurement	Attestation	CPU Isolation	Memory Isolation
Intel SGX	Immutable	Mutable	Mutable	Mutable	Mutable + Immutable
Intel TDX	Immutable	Mutable	Mutable	Mutable	Mutable
AMD SEV-SNP	Immutable	Unknown	Mutable	Unknown	Unknown
Sanctum	Immutable	Mutable	Mutable	Mutable	Mutable
Iso-X	Immutable	Immutable	Immutable	Immutable	Immutable

Most TEEs use immutable RTM but mutable components for other security functions. Few designs like Iso-X implement everything in immutable hardware.