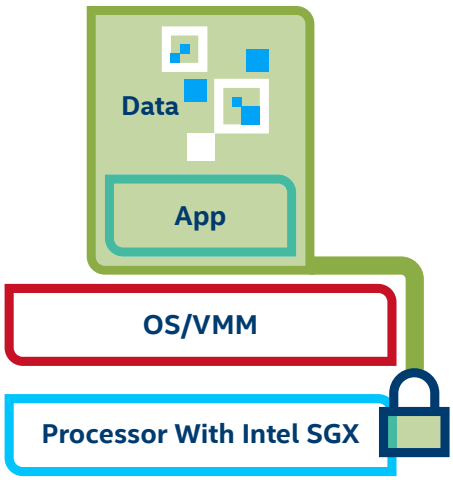
Product Brief

Intel Platform Security Technologies
Intel® Software Guard Extensions (Intel® SGX)

Enhanced Security Features for Confidential Computing

Data security using new hardware-based controls



Intel® SGX enables confidential computing solutions that allow you to unlock the secrets within your siloed data or collaborate with partners and other organizations while keeping everyone's data private—regardless of where that data sits.

Enhances Confidentiality and Integrity
Protects sensitive data even in the presence of privileged malware at the OS, BIOS, VMM, or SMM layers.

Choice in How You Deploy
Run your existing application with an SGX library OS or develop purpose-built applications with a range of available SDKs.

Remotely Attest and Provision
A relying part can verify an application enclave's identity and enhance security of provisioning keys, credentials, and other sensitive data in the enclave.

Reduce Attack Size
Bypassing the OS and VM, applications can communicate directly with the CPU.

"Thanks to the Intel SGX technology, we can verify that the piece of code running on someone else's computer is the same piece of code running on your computer—and we use that knowledge to build a trusted system."

Shane Glynn,
Cofounder and General Counsel,
MobileCoin

The Confidential Computing Challenge

Until recently, security has focused just on encrypting data that is at-rest in storage or being transmitted on a network, but not protecting data while it is in use. Intel SGX leverages the strengths of the CPU platform and builds on a foundation of security to protect data and applications while in use.

Intel SGX – Getting Started

If you have an existing application that you want to use with Intel SGX, you just need to use an open-source Library OS (LibOS) solution like Gramine-SGX or any of the other commercial SGX LibOS offerings available. LibOS's are lightweight OS's that maintain SGX security boundaries and that can be easily deployed to a cloud service provider (CSP) that supports Intel SGX or deployed in a company's data center on Intel SGX-enabled servers.

For new application development, you can pick from a variety of SDKs that support Intel SGX. The Intel SGX SDK and the Confidential Computing Consortium's Open Enclave SDK are two examples.

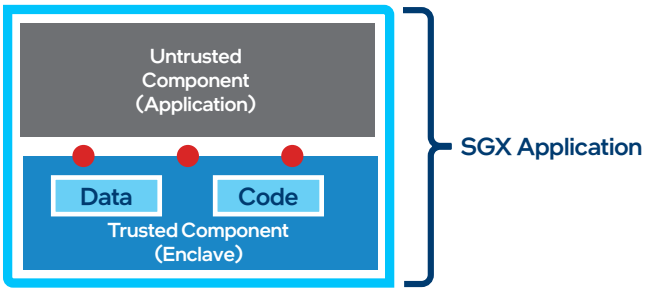


Figure 2: Application Partitioning Example

Figure 2 shows an example of an Intel SGX application that includes two parts: an untrusted part that launches the enclave, and a trusted part where production code runs in an enclave. A developer can create multiple enclaves that work in concert to support distributed architectures.

Many solutions benefit from the additional protection provided by Intel SGX. Solution examples include privacy preserving AI and ML processing, key management, proprietary algorithms, protection of biometrics, etc.

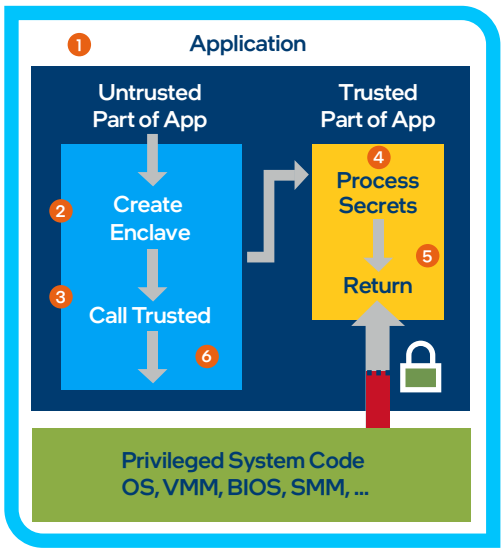


Figure 3: Runtime Execution

1. App built with trusted (enclave) and untrusted parts
2. App runs and creates the enclave, which is placed in trusted memory
3. Trusted function is called, execution transitioned to the enclave
4. Enclave sees all process data in clear; the technology helps to deny external access to enclave data
5. Trusted function returns; enclave data remains in trusted memory
6. Application continues normal execution

In this example, at runtime (see Figure 3), the Intel SGX instructions build and execute the enclave inside a special encrypted memory region with restricted entry/exit locations defined by the developer. This helps prevent data leakage: data is only in plain-text when it is isolated and protected by the SGX enclave. Upon exit from the enclave, it is encrypted. Snoops on the memory bus or system memory will find only cypher-text.

> "Using Intel SGX has allowed us to build a platform that can securely and privately process data from a variety of partners. This allows us to all collaborate better and create more effective advertising campaigns for customers."
>
> Fabian Schaefer,
> Director of Analytics and Data Management, Magnit

Attesting Enclaves and Sealing Data

Currently, device manufacturers and ISVs commonly provision application software and secrets at manufacturing time or via complex field configurations that cannot cryptographically prove application integrity. Intel SGX enables local attestation between enclaves running on the same platform by attesting to the relying party that their enclave is running in an expected HW/SW config. The relying application receives confirmation that the enclave it is interacting with is running as expected and proceeds normally.

The trusted portion of an application is loaded into an enclave where its code and data are measured. An enclave report is signed by an Attestation Key and sent to the relying party, which in turn can validate that the enclave report was generated by an authentic Intel® processor. (See Figure 4). Upon verification of the enclave identity, the relying party can have more trust in the enclave and provision keys, credentials, or other data.

Figure 4: Attestation and Sealing

Intel SGX includes an instruction for generating a CPU/platform and/or enclave-specific "Sealing Key" that can be used to more safely store and retrieve sensitive information that may need to be stored to disk or protected while outside the enclave.

Data Center Attestation

Intel® SGX Data Center Attestation Primitives (Intel® SGX DCAP) (see Figure 5) allows the enterprise, data center, and cloud service providers to build and deliver an attestation service themselves, rather than using the remote attestation from a 3rd party provider. This also removes the need for direct Internet access and allows all provisioning and quote verification to remain on the local network.

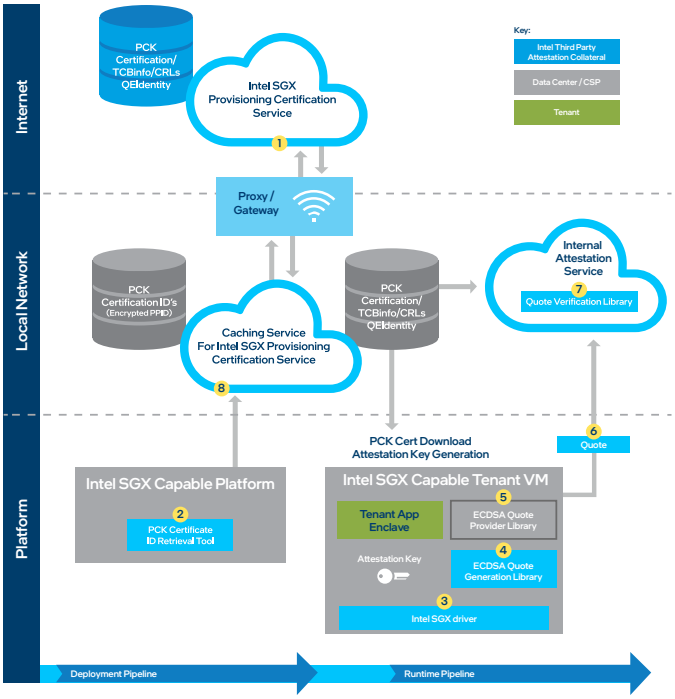


Figure 5: Intel® SGX Data Center Attestation Primitives

Intel SGX Helps Enable New Security Models and Innovation

The foundational capability of Intel SGX is to help enable software to be significantly less vulnerable to attacks by providing a higher level of isolation and attestation for program code, data and critical IP from the OS, applications, and hardware on the platform. Intel SGX has been used to help enhance security within multiple use cases and applications. Examples of these applications are listed on the following page.

Use Cases

Artificial Intelligence (AI)/Machine Learning (ML)
Protect your AI and ML workloads and applications while they are running.

Cloud Infrastructure
Confidentiality of customer applications and workloads in public cloud infrastructures.

Trusted Multi-Party Compute/ Multi-Party Analytics
Enable multiple parties to collaborate on shared data while keeping sensitive data confidential.

Secure Key Management
Use enclaves to help protect cryptographic keys and provide HSM-like functionality.

Blockchain
Increase privacy and security for transaction processing, consensus, smart contracts, and key storage.

Network Function Virtualization
Establish trust for virtualized network functions.

Intel SGX Resources

Intel SGX
http://Intel.com/SGX

Intel Developer Zone (IDZ) – SGX
http://software.intel.com/sgx

Intel Data Center Attestation Primitives (DCAP) and Intel SGX SDK
https://01.org/intel-software-guard-extensions

Specifications

Required Hardware	Supported Development Software	SGX-compatible OSs
Intel® Xeon® 3rd generation Scalable platform	**Windows:**	**Windows:**
Intel® Xeon® processor E3-1500 v5 and v6	Microsoft Visual Studio 2019	Window 10
Intel® Xeon® processor E family 2100	**Linux:**	Windows Server
	GNU toolchain	**Linux:**
	Intel® SGX Eclipse Plug-in	Ubuntu
		Red Hat
		Fedora
		SUSE
		CentOS
		To find the latest pre-built binaries that reflect specific OS support, go to: https://01.org/intel-software-guard-extensions/downloads

For the latest information on Intel SGX go to: intel.com/sgx