WHITE PAPER

Intel® Software Guard Extensions (Intel® SGX)

Intel Integrated Performance Primitives in Intel® SGX Applications

Introduction

The Intel® Software Guard Extensions (Intel® SGX) SDK incorporates the Intel® Integrated Performance Primitives (Intel® IPP) Cryptography library. This article provides basic information on this Intel IPP Cryptography library and how to get set up to use it with Windows* Visual Studio* and the Linux* OS.

In the Intel SGX SDK, the **sgx_tcrypto** library is linked to Intel's IPP Cryptography library. For Windows, the header files are also included in the SDK, which allows direct access to the Intel IPP Cryptography library API. (For Linux, the header files are downloaded and installed manually.) Figure 1 shows the relationship of the Intel IPP Cryptography library to the **sgx_tcrypto** library.

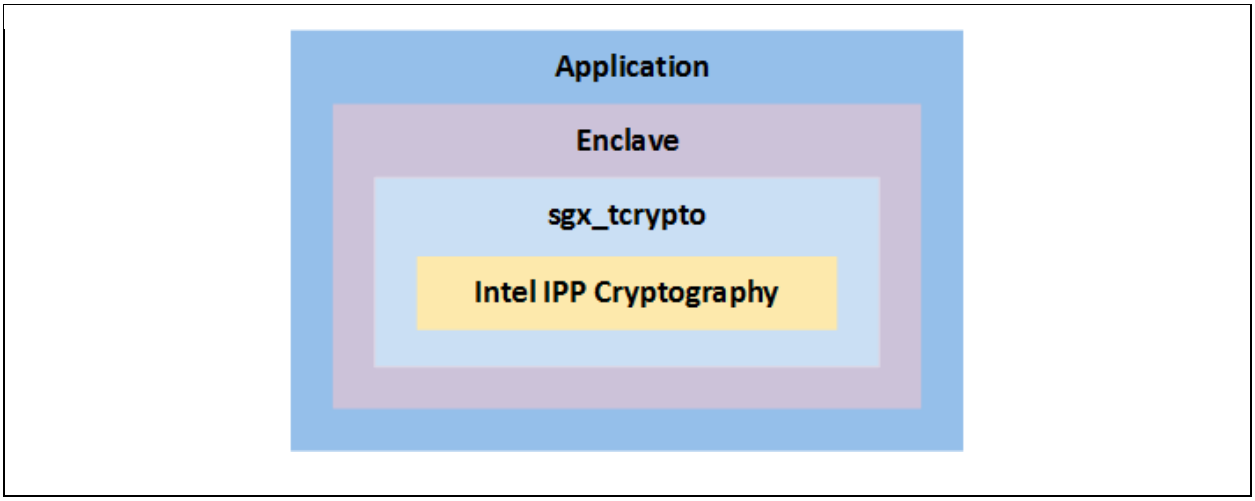

Figure 1. Intel IPP Cryptography library used in Intel SGX enclave

Notes:

- The Intel IPP Cryptography library included in the Intel SGX SDK supports 2 optimization levels only to reduce enclave size and minimize EPC consumption:
  - Intel® Streaming SIMD Extensions 4.1 (Intel SSE4.1)/Intel® Streaming SIMD Extensions 4.2 (Intel SSE4.2)/Intel® Advanced Encryption Standard–New Instructions (Intel AES-NI)
  - Intel® Advanced Vector Extensions 2 (Intel AVX2)
- All processors that support Intel SGX also support Intel SSE4.1/Intel SSE4.2/Intel AES-NI, which support constant timing. Some processors that support Intel SGX also support Intel

AVX2. If Intel AVX 2 is not supported by a processor, the Intel IPP Cryptography library defaults to the Intel SSE4.1/Intel SSE4.2/Intel AES-NI implementation.

Details on Intel's IPP library can be found https://software.intel.com/en-us/intel-ipp.

A complete list of Intel IPP Cryptography features is available at https://software.intel.com/en-us/ipp-crypto-reference.

Accessing the Intel IPP Cryptography Library

Visual Studio

Follow these guidelines to access this library support in Visual Studio:

1. Download and install the Intel SGX SDK for Windows.
2. Ensure that your Intel SGX enclave project links to `sgx_tcrypto`.
3. Add the Intel IPP Cryptography header file path `$(SGXSDKInstallPath)\include\ipp` to the project settings.
4. Add the header file (`ippcp.h`) to the enclave source for your Intel SGX application.

Intel IPP Crypto calls from the application will now be resolved by the Intel SGX Cryptography library.

Linux

Follow these guidelines to make use of this library support with Linux:

1. Download and install the Intel SGX SDK for Linux.
2. Download and install the Intel IPP Library.
3. Download and install the Intel IPP Cryptography Library.
4. Ensure that your Intel SGX enclave project links to `sgx_tcrypto`.
5. Add the Intel IPP Cryptography header file path `(/opt/intel/ipp/include)` to the enclave project settings.
6. Add the header file (`ippcp.h`) to the enclave source for your Intel SGX application.

Intel IPP Crypto calls from the application will now be resolved by the Intel SGX Cryptography library.