

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.

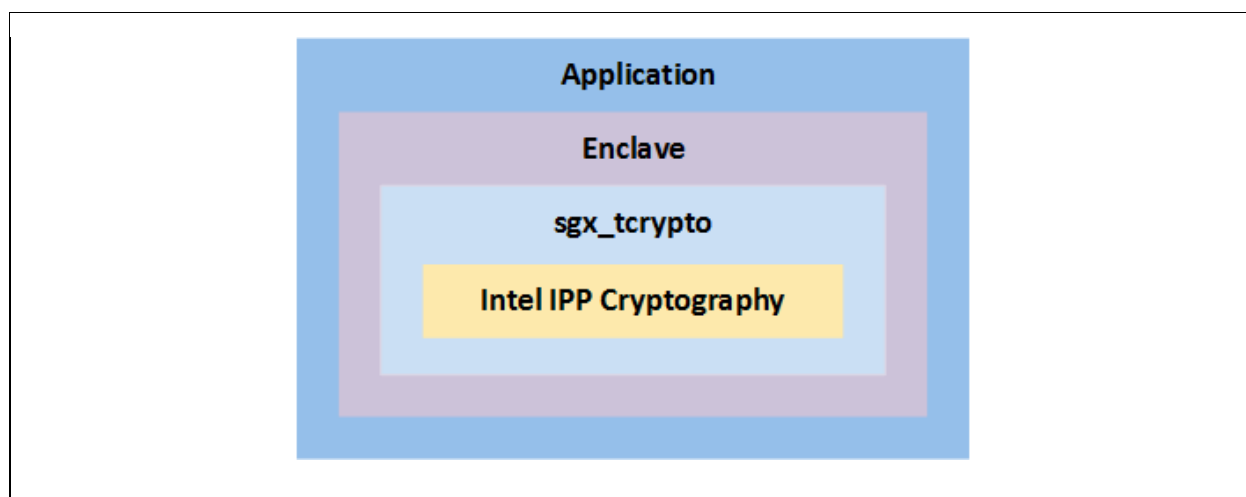


Figure 1. Intel IPP Cryptography library used in Intel SGX enclave

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

Intel® Software Guard Extensions (Intel® SGX)

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.

Intel® Software Guard Extensions (Intel® SGX)

INFORMATION IN THIS DOCUMENT IS PROVIDED IN CONNECTION WITH INTEL® PRODUCTS. NO LICENSE, EXPRESS OR IMPLIED, BY ESTOPPEL OR OTHERWISE, TO ANY INTELLECTUAL PROPERTY RIGHTS IS GRANTED BY THIS DOCUMENT. EXCEPT AS PROVIDED IN INTEL'S TERMS AND CONDITIONS OF SALE FOR SUCH PRODUCTS, INTEL® ASSUMES NO LIABILITY WHATSOEVER AND INTEL® DISCLAIMS ANY EXPRESS OR IMPLIED WARRANTY, RELATING TO SALE AND/OR USE OF INTEL® PRODUCTS INCLUDING LIABILITY OR WARRANTIES RELATING TO FITNESS FOR A PARTICULAR PURPOSE, MERCHANTABILITY, OR INFRINGEMENT OF ANY PATENT, COPYRIGHT OR OTHER INTELLECTUAL PROPERTY RIGHT.

A "Mission Critical Application" is any application in which failure of the Intel Product could result, directly or indirectly, in personal injury or death. SHOULD YOU PURCHASE OR USE INTEL'S PRODUCTS FOR ANY SUCH MISSION CRITICAL APPLICATION, YOU SHALL INDEMNIFY AND HOLD INTEL® AND ITS SUBSIDIARIES, SUBCONTRACTORS AND AFFILIATES, AND THE DIRECTORS, OFFICERS, AND EMPLOYEES OF EACH, HARMLESS AGAINST ALL CLAIMS COSTS, DAMAGES, AND EXPENSES AND REASONABLE ATTORNEYS' FEES ARISING OUT OF, DIRECTLY OR INDIRECTLY, ANY CLAIM OF PRODUCT LIABILITY, PERSONAL INJURY, OR DEATH ARISING IN ANY WAY OUT OF SUCH MISSION CRITICAL APPLICATION, WHETHER OR NOT INTEL® OR ITS SUBCONTRACTOR WAS NEGLIGENT IN THE DESIGN, MANUFACTURE, OR WARNING OF THE INTEL® PRODUCT OR ANY OF ITS PARTS.

Intel may make changes to specifications and product descriptions at any time, without notice. Designers must not rely on the absence or characteristics of any features or instructions marked "reserved" or "undefined". Intel reserves these for future definition and shall have no responsibility whatsoever for conflicts or incompatibilities arising from future changes to them. The information here is subject to change without notice. Do not finalize a design with this information.

No computer system can provide absolute security under all conditions. Built-in security features available on select Intel® processors may require additional software, hardware, services and/or an Internet connection. Results may vary depending upon configuration. Consult your system manufacturer for more details.

Intel®, the Intel® Logo, Intel® Inside, Intel® Core™, Intel® Atom™, and Intel® Xeon® are trademarks of Intel Corporation in the U.S. and/or other countries. Other names and brands may be claimed as the property of others.

* Other names and brands may be claimed as properties of others.

Copyright © 2017 Intel® Corporation