Intel® Software Guard Extensions SSL (Intel® SGX SSL) Library

Architecture

Legal Information

No license (express or implied, by estoppel or otherwise) to any intellectual property rights is granted by this document.

Intel disclaims all express and implied warranties, including without limitation, the implied warranties of merchantability, fitness for a particular purpose, and non-infringement, as well as any warranty arising from course of performance, course of dealing, or usage in trade.

This document contains information on products, services and/or processes in development. All information provided here is subject to change without notice. Contact your Intel representative to obtain the latest forecast, schedule, specifications and roadmaps.

The products and services described may contain defects or errors known as errata which may cause deviations from published specifications. Current characterized errata are available on request.

Intel technologies features and benefits depend on system configuration and may require enabled hardware, software or service activation. Learn more at Intel.com, or from the OEM or retailer.

Copies of documents which have an order number and are referenced in this document may be obtained by calling 1-800-548-4725 or by visiting www.intel.com/design/literature.htm.

Intel, the Intel logo, Xeon, and Xeon Phi 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.

Table of Contents

Intel® Software Guard Extensions SSL Library

The Intel® SGX SSL cryptographic library is intended to provide cryptographic services for Intel® Software Guard Extensions (Intel® SGX) enclave applications.

The Intel® SGX SSL cryptographic library is based on the underlying OpenSSL* Open Source project, providing a full-strength general purpose cryptography library.

The API exposed by the Intel® SGX SSL library is fully compliant with unmodified OpenSSL APIs.

NOTE: Only a specific subset of APIs available in OpenSSL is supported by the Intel® SGX SSL cryptographic library.
Unsupported OpenSSL APIs included in the Intel® SGX SSL cryptographic library are not validated or recommended. See Appendix A for the supported OpenSSL APIs in the developer guide.

In addition, the Intel® SGX SSL library exposes a closed set of manageability APIs, a list of which is provided in Supported APIs in the developer guide.

1.1. Terminology

Term	Description
Intel® SGX	Intel® Software Guard Extensions
EDL	Enclave Definition Language. EDL files define the enclave interface for trusted-to-untrusted and untrusted-to-trusted transitions.

1.2. Legal Considerations

The Intel® SGX SSL Library is based on the OpenSSL* open source libraries licensed under a dual license, i.e. both the conditions of the OpenSSL license and the original SSLeay license apply.

More information regarding the OpenSSL license is available at https://www.openssl.org/source/license.html

You MUST be aware of license requirements and/or limitations of the underlying OpenSSL library and fully conform to it.

NOTE: This product includes software developed by the OpenSSL Project for use in the OpenSSL Toolkit (https://www.openssl.org)

1.3. Architecture Overview

The Intel® SGX SSL library consists of the following components:

- Intel® SGX SSL cryptographic library representing OpenSSL* 1.1.0 cryptographic library built to run inside an enclave.
- A trusted library providing implementation for missing system APIs inside an enclave.
- An untrusted library providing implementation of missing system APIs outside an enclave.

The following figure shows how Intel® SGX SSL library is used in an Intel® SGX application.
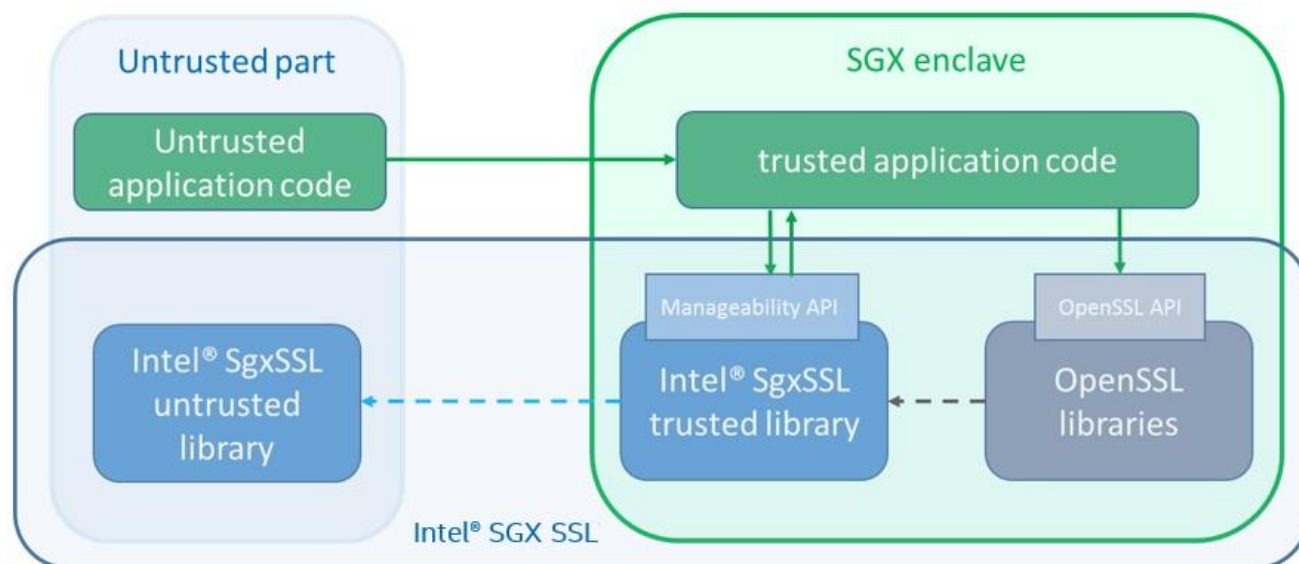

Figure 1 Intel® SGX SSL library Usage

Here is the flow of execution as illustrated in Figure 1:

1. The user's untrusted application code calls the trusted code with a function declared in the EDL file

2. The user's trusted code may use manageability API for different purposes, like to get Intel® SGX SSL library version, to register a callback function to intercept the Intel® SGX SSL libraries printout messages, and so on.

3. The user's trusted code continues execution and at a certain point calls an API supported by the Intel® SGX SSL cryptographic or TLS libraries. The supported API is a subset of the unmodified OpenSSL API.

4. The call is passed to the Intel® SGX SSL cryptographic library. Some functions are internal and do not rely on system APIs (for example, SHA256), so the functions complete and return.

5. Other functions require some system APIs, so the execution passes to the Intel® SGX SSL trusted library code that implements them. If the system API can be implemented internally (for example, pthread_once), it returns after completion without leaving the enclave.

6. Other APIs must leave the trusted code and are executed in the untrusted area (for example, ftime)

On an S3/S4 power event the internal state of the operation (for instance, during BASE64 encode/decode API usage) executed by the Intel® SGX SSL library will be lost as part of the entire enclave loss. The Intel® SGX SSL library does not manage saving or restoring the state on suspend or resume operations. It is the customer's application responsibility to save an internal Intel® SGX SSL state on suspend and to restore it on resume when applicable.

1.4. Security Recommendations.

Intel® SGX SSL provides support for OpenSSL* inside an enclave. Security assets, like cryptographic keys, client certificate private keys, and plain data (both network traffic and cryptographic payload) do not need to leave an enclave. Thus they are protected by the Intel® SGX technology. Intel® SGX SSL library provides integrity and confidentiality of security assets and protects them from both malicious software and a simple hardware attack.

Intel® SGX SSL library relies on an implementation of OpenSSL and Intel® SGX to handle side channel attacks. Our architecture is designed to not leak additional information through the OCALLs, but it doesn't protect against side channel attacks. So, in case of side channel attacks it is as secure OpenSSL without Intel® SGX.

Getting current system time is not supported inside an enclave and is therefore implemented by Intel® SGX SSL library as OCALL. This approach allows an attacker to manipulate the time values coming from an untrusted component. Time values are used by Intel® SGX SSL library for time related certificate verification checks as well as for TLS session expiration checks. To reduce the risk of a time attack on an enclave application that uses the Intel® SGX SSL, we recommend you use server certificate pinning.

An enclave application, built with Intel® SGX SSL library, is responsible for preserving the protection features of Intel® SGX SSL library. Follow the listed expectations of and recommendations for the customer enclave application:

- The customer's application is responsible to build production enclave as non-debug enclave.
- The customer's application should utilize Intel® SGX architecture and Intel® SGX software to protect security assets. For instance, the customer's application should use certificate pinning. Server certificate should be provisioned into an enclave and protected by enclave sealing capabilities.
- The customer's application should not expose security assets by trusted to untrusted transitions
- The customer's application should sanitize input data coming from untrusted components
- The customer's application should configure Intel® SGX SSL not to support obsolete protocols and cryptographic suites
- The customer's application should use only the OpenSSL APIs that are supported by the Intel® SGX SSL library.
- The customer's application should use OpenSSL APIs correctly to verify server certificate.