Intel® SGX Product Licensing

Submitted by Dinesh Rao (Intel) (https://software.intel.com/en-us/user/334958) on February 28, 2016

The Intel® SGX SDK for Windows was recently made available (https://software.intel.com/sgx-sdk) on the Intel Developer Zone site. The SDK is provided under an evaluation license. Since the release of the SDK, we've received a number of inquiries about getting a production license for Intel® SGX. While the particulars of the production license agreement are fairly routine, it might be helpful to those that have expressed an interest to get a better sense of the context within which production license requests are considered.

Developers should first consider whether a production license is necessary. Intel® SGX is a CPU-based technology that allows developers to protect select portions of an application. This protection is based on the use of Intel® SGX enclaves. With the Intel® SGX SDK for Windows, it is possible to create debug enclaves. A good description of the range of possibilities offered by debug enclaves is provided in this blog (https://software.intel.com/en-us/blogs/2016/01/07/intel-sgx-debug-production-prelease-whats-the-difference) by SGX Program Architect Simon Johnson. It can be inferred from Simon's blog that a production license is required when developers plan to ship commercial software that needs to keep enclaved code confidential.

This brings us back to the topic of considerations that factor into evaluating production license requests. Since the ability to launch an enclave puts developers in a position of trust on a given platform, Intel assesses the ability of applicants for production licenses to meet critical security requirements underpinning the use of Intel® SGX.

While not a complete list, the three areas below outline some key expectations of production license recipients. Applicants should note that this list is not exhaustive and there may be additional requirements that must be fulfilled prior to being granted a production license. At a minimum, potential licensees must have a demonstrated ability to perform:

1. *Secure Software Development*: Licensees must use good development techniques and programming practices, including those highlighted in the Intel ® SGX Enclave Writers Guide that accompanies the Intel® SGX SDK. In addition, licensees must follow secure coding practices to avoid vulnerabilities; agree to notify Intel of, and fix, vulnerabilities within a pre-defined time; re-distribute and keep current the Intel® SGX Platform Software included with their SGX-enhanced application; and undertake not to write malware, spyware, nuisance-ware or fail to deliver on the security promise implied by the use of Intel® SGX enclaves. Applications that may consume all available enclave memory, impact system stability, or affect user experience as a result of inability to launch their enclave(s) may require significant investigation and discussion. The ability to uninstall licensee applications, upon user request, must be complete, including the removal of sealed data.
2. *Enclave Signing Key Management*: Developers requesting a Production License must demonstrate the ability to protect their enclave signing key and have a security protocol/program in place which accords with industry best practices for key management (https://www.thawte.com/code-signing/whitepaper/best-practices-for-code-signing-certificates.pdf). At a minimum, potential licensees must have information security procedures in place which implement the following requirements:
   Licensees should implement the principle of least privilege (multi-factor authentication for access, blocking unused ports, installing all security updates, running an updated AV scanner, separating networks and credentials used for development systems from other computing systems) for development and key management systems; ensure that code testing minimizes exposure of private keys and signing mechanisms by using an internal test signing Certificate Authority; set up a parallel code signing infrastructure for developers to use that internal CA; store keys in a secure, tamper-proof, cryptographic hardware device such as an HSM; and implement physical security measures (cameras, guards, fingerprint scanners, background checks) to protect against theft (by insiders and infiltrators), compromise, and abuse. Licensees must agree to notify Intel of any breach, loss or theft of their enclave signing key within a predefined time.
3. *Relying Party Functions*: Licensees will act as a relying party to the Intel Attestation Verification Service. As a result, licensees will be required to demonstrate their ability to manage, update, and control application servers that deliver Intel® SGX enhanced applications to capable platforms. These application servers must comply with the requirements (SLAs, rate limiting, usage limits, DDoS prevention, etc.) of the Development and Production versions of the Intel Attestation Verification Service. Relying party functionality relative to the Intel Attestation Verification Service includes the ability to process Linkable and Anonymous Quotes and to deliver updates of the Intel® SGX Platform Software.

With this context in mind, developers who want to ship commercial software that uses Intel® SGX should contact the SGX Program (mailto:sgx_program@intel.com) to initiate the process of applying for a production license as soon as they are:

1. Ready to provide a detailed description of the application and intended SGX use case(s) and prepared to answer detailed follow-up questions.
2. Able to demonstrate to Intel's satisfaction that they have business processes and controls in place to meet or exceed the security requirements described above.

Intel will provide a non-disclosure agreement to cover the information above if we do not already have one in place with your company.

For more complete information about compiler optimizations, see our Optimization Notice (/en-us/articles/optimization-notice#opt-en).

Categories: Security (/en-us/search/site/field_topic/security-20870/language/en) , Software Guard Extensions (/en-us/search/site/field_technology/software_guard_extensions-43865/language/en)

Add a Comment

Top

(For technical discussions visit our developer forums. For site or software product issues contact support.)

Please sign in to add a comment. Not a member? Join today ›