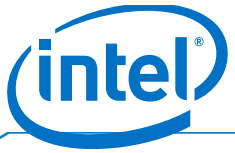
Technical Note

Intel® SGX Attestation Technical Details



Intel® SGX Technical Details for INTEL-SA-00219 and INTEL-SA-00220

One way to ensure that Intel® SGX platforms have been appropriately updated is through the process of attestation. The attestation process verifies that the platform is a valid Intel® SGX platform and the platform components meet a defined set of security requirements. In addition, the attestation process enables the application provider to verify the security version of the application.

Intel will perform a TCB Recovery operation to enable parties utilizing Intel® SGX to determine whether the updates (microcode and SGX Platform Software) for these vulnerabilities have been applied on the platform the attestation request originated from. API version 3 for the Intel® SGX Attestation Service (IAS) is required to use attestation. For details on IAS API, please refer to the IAS API Version 3 Specification.

- On 12/03/2019, these updates will be applied to the Intel® SGX Attestation Service (DEV environment), and on 01/07/2020, they will be applied to the IAS Production Environment (LIV).
- The "GROUP_OUT_OF_DATE" response is returned for platforms without the BIOS applied microcode update or the SGX Platform Software version required.
- An attestation response may report a "CONFIGURATION_NEEDED" for platforms that have applied the microcode update and SGX platform software where the integrated processor graphics technology remains enabled. The Remote Attestation Verifier should evaluate the potential risk of an attack on these platforms.
- An attestation response may still report a "CONFIGURATION_NEEDED" for attestation requests originating from Intel® SGX enabled platforms that updated that have applied the microcode and SGX platform software update, where the platform's configuration does not meet requirements identified in INTEL-SA-00161 or INTEL-SA-00233 impacting Intel® SGX. The Remote Attestation Verifier should evaluate the potential risk of an attack on these platforms.

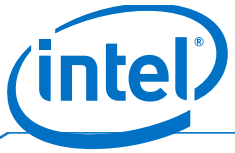
For Intel® SGX environments that are supporting the construction of their own attestation infrastructure with the Intel® SGX Platform Certificate Retrieval Service, updated certificates that reflect the enablement status of Intel® SGX will be generated.

Further TCB Recovery Guidance for developers is available.

Revision	Date	Description
1.0	11/12/2019	Initial Release

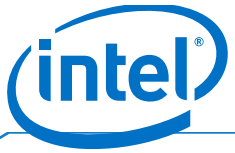
Technical Note

Intel® SGX Attestation Technical Details



Technical Note

Intel® SGX Attestation Technical Details



Legal Notices and Disclaimers

Intel provides these materials as-is, with no express or implied warranties.

All products, dates, and figures specified are preliminary based on current expectations, and are subject to change without notice.

Intel products and services described may contain design defects or errors known as errata, which may cause the product to deviate 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. Performance varies depending on system configuration. No product or component can be absolutely secure. Check with your system manufacturer or retailer or learn more at http://intel.com.

Some results have been estimated or simulated using internal Intel analysis or architecture simulation or modeling, and provided to you for informational purposes. Any differences in your system hardware, software or configuration may affect your actual performance.

Intel and the Intel logo are trademarks of Intel Corporation or its subsidiaries in the United States and other countries.

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