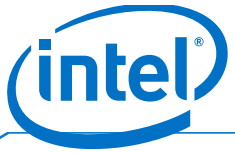
Technical Note

Intel® SGX Attestation Technical Details



Intel® SGX Technical Details for INTEL-SA-00320 and INTEL-SA-00329

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.

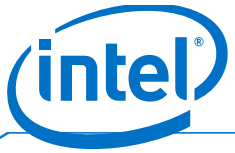
Intel will perform a TCB Recovery operation to enable parties utilizing Intel® SGX to determine whether the updates (microcode) for these vulnerabilities have been applied on the platform from which the attestation request originated.

- On June 16, 2020, the updates listed below will be enabled in the IAS Development Environment (DEV), and on July 14, 2020 they will be enabled in the IAS Production Environment (LIV).
- A "GROUP_OUT_OF_DATE" response is returned for platforms without the required, BIOS-applied microcode update.
- An attestation response may still report "SW_HARDENING_NEEDED", "CONFIGURATION_NEEDED" or "CONFIGURATION_AND_SW_HARDENING_NEEDED". This happens for attestation requests originating from Intel® SGX-enabled platforms that have applied the microcode update, but where the platform's configuration does not meet requirements identified in INTEL-SA-00161, INTEL-SA-00233 , INTEL-SA-00219 and INTEL-SA-00289 or where the platform is affected by INTEL-SA-00334

For Intel® SGX environments that are supporting the construction of their own attestation infrastructure with the Intel® SGX Platform Certificate Retrieval Service, updated verification collateral will be provided.

Further TCB Recovery Guidance for developers is available.

Revision	Date	Description
1.0	6/9/2020	Initial release



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.

© Intel Corporation.