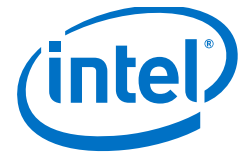


# Technical Note

Intel® SGX Attestation Technical Details



## Intel® SGX Technical Details for INTEL-SA-00289 and INTEL-SA-00334

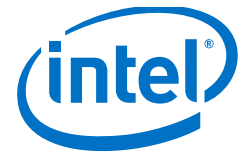
One way to ensure that Intel® SGX platforms have been appropriately updated is through the process of attestation. The attestation process verifies that the platform is a valid Intel® SGX platform and the platform components meet a defined set of security requirements. In addition, the attestation process 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 from which the attestation request originated and whether the platform is affected by [INTEL-SA-00334](#). API version 4 for the Intel® SGX Attestation Service (IAS) is required to receive information about whether the platform is affected by INTEL\_SA\_00334, Intel® SGX Attestation Service (IAS) API version 3 will not report whether the platform is affected by INTEL-SA-00334. For details on IAS API, please refer to the [IAS API Specification](#).

- On **March 17, 2020**, API version 4 and the updates listed below will be enabled in the IAS Development Environment (DEV), and on **April 14, 2020** they will be enabled in the IAS Production Environment (LIV).
- A "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 "SW\_HARDENING\_NEEDED" for attestation requests originating from Intel® SGX-enabled platforms that have applied the microcode and SGX platform software update and are properly configured but are affected by INTEL-SA-00334. In this case a Remote Attestation Verifier should evaluate the potential risk of an attack on these platforms and whether the attesting enclave employs adequate software hardening to mitigate the risk.
- An attestation response may report "CONFIGURATION\_NEEDED" or "CONFIGURATION\_AND\_SW\_HARDENING\_NEEDED" for attestation requests originating from Intel® SGX-enabled platforms affected by [INTEL-SA-00289](#) that have applied the microcode update, but where the BIOS did not disable the interface the privileged software can cause undervoltage to the processor. The "CONFIGURATION\_NEEDED" response implies the platform is not affected by INTEL-SA-00334, while "CONFIGURATION\_AND\_SW\_HARDENING\_NEEDED" indicates the platform is affected by INTEL\_SA\_00334.

# Technical Note

Intel® SGX Attestation Technical Details



- An attestation response may still report “CONFIGURATION\_NEEDED” or “CONFIGURATION\_AND\_SW\_HARDENING\_NEEDED” for attestation requests originating from Intel® SGX-enabled platforms that have applied the microcode and SGX platform software update, but where the platform’s configuration does not meet requirements identified in [INTEL-SA-00161](#), [INTEL-SA-00233](#) and [INTEL-SA-00219](#). Again “CONFIGURATION\_NEEDED” only response implies the platform is not 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 reflecting whether the platform is affected by INTEL-SA-00334 will be provided.

Further [TCB Recovery Guidance](#) for developers is available.

Revision	Date	Description
0.1	1/14/2020	Initial draft

## 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.