Attestation Service for Intel® Software Guard Extensions (Intel® SGX): API Documentation

Revision: 6.0

1 Abbreviations

Abbreviation	Description
IAS	Attestation Service for Intel® SGX
CA	Certificate Authority
EOL	End of Life
EPID	Enhanced Privacy ID
JSON	JavaScript Object Notation
MTLS	Mutual Transport Layer Security
QE	Quoting Enclave
REST	Representational State Transfer
SP	Service Provider
TCB	Trusted Computing Base
TLV	Type-length-value
UUID	Universally Unique Identifier
{*variable*}	Denotes a variable parameter in the API

2 Attestation Service for Intel® SGX

Attestation Service for Intel® SGX (IAS) is a web service hosted and operated by Intel in a cloud environment. The primary responsibility of the IAS is verification of attestation evidence submitted by Service Providers (SPs).

2.1 Registering for the Service

Registration of Service Providers (SPs) to IAS is handled via API web portal.

Note: *The previous method of registering for the Service that included submitting a form with x.509 client certificate, email address, and Linkable/Unlinkable EPID signatures policy has been replaced by the self-service API portal, and will no longer available. Existing users of the Service who registered using x.509 client certificate are not expected to migrate to the API portal at this time. Explicit communication regarding the transition to the portal will be communicated directly to users along with timelines for deprecation of existing infrastructure. Users registered with x.509 client certificates can access the Rev 4.1 version of this specification here.*

Subscribing to IAS API requires Service Provider to be logged in to the portal using Intel® Developer Zone account. Service Providers that do not have an Intel® Developer Zone account can create one using a "Sign up" link on the portal.

Upon successful login, Service Provider can subscribe to IAS API. Successful subscription provides Service Provider with the following artifacts required to use the API:

- ***Service Provider ID (SPID)*** – unique identifier of Service Provider for given API. SPID value needs to be provided in the first 16 bytes of BASENAME field in Quote structure.
- ***Subscription Key*** – unique API key that Service Provider needs to use to authenticate itself to the service. Subscription Key needs to be provided in the header of each request sent to IAS. Confidentiality of Subscription Key in the request is protected by encrypted connection to the service (over HTTPS). IAS will reject any requests with no or unrecognized Subscription Key.

Note: *Subscription Key is a credential to access the API. It is known only to the owner (i.e. Service Provider) and it is the responsibility of the owner to protect its confidentiality. API portal allows for an on-demand rotation of the keys to support custom key rotation policies.*

Email address provided during the registration might be used to notify the Service Provider about updates and availability of IAS (for example, planned and unplanned downtimes, limited availability alerts) as well as revocation data updates. In certain cases, it may be beneficial that the provided email address is that of a publicly addressable enterprise distribution list so that the enterprise can manage who receives notifications (for example, engineering, operations and others).

2.2 Supported Environments

Development Environment – test environment established for software development purposes such as early developer integration. Accessing the environment does not require any additional approvals from Intel.

Base URL: https://api.trustedservices.intel.com/sgx/dev

Production Environment – production-quality environment to be used by production ready software. Accessing the environment requires submitting a form and getting an approval from Intel.

Base URL: https://api.trustedservices.intel.com/sgx

2.3 Authentication

Attestation Service for Intel® SGX exposes its APIs over HTTPS protocol (based on TLS) and requires both client and server authentication.

2.3.1 Supported TLS Versions

Attestation Service for Intel® SGX only accepts connections protected by TLS 1.2 or higher. IAS drops any incoming connections utilizing SSL protocol in any version.

2.3.2 Server Authentication

Server authenticates itself using a standard x.509 certificate issued by commonly trusted Certificate Authority (CA) during Transport Layer Security (TLS) session establishment.

2.3.3 Client Authentication

Clients authenticate themselves using a Subscription Key provided in HTTP header (Ocp-Apim-Subscription-Key) in each HTTP request made to the Service. An encrypted TLS session protects Confidentiality of the Subscription Key. Subscription Keys can be obtained from the API portal. Refer to Section 2.1 in this document for more information.

2.4 Available API Versions

The latest available API version exposed by Attestation Service for Intel® SGX is version 4. Previous versions of Attestation API are considered deprecated. This document focuses only on API version 4. Users of API version 3 can access the Rev 5.0 version of this specification here.

2.4.1 Summary of API v4 Changes

The changes introduced in Attestation API version 4 mainly focus on the following areas:

1. Verify Attestation Evidence API was updated, specifically there is a new version of Attestation Verification Report (version 4) with new statuses (SW_HARDENING_NEEDED and CONFIGURATION_AND_SW_HARDENING_NEEDED) added to isvEnclaveQuoteStatus (see Section 4.2.1 for further details).
2. Security Advisory IDs (described by advisoryURL and advisoryIDs) have been moved from headers returned together with the Attestation Verification Report to the report itself (see Section 3.2.2 and Section 4.2.1 for further details).

2.5 Troubleshooting

Each HTTP call to the API results in a response, containing a header called *Request-ID.* The value of *Request-ID* contains a randomly generated Universally Unique Identifier (UUID) that can be used to track an individual HTTP request. In case of an error, the value of this header should be logged by the SP and included in the issue submission so that further troubleshooting is possible.

3 Attestation API (version 4)

The Attestation API exposed by Attestation Service for Intel® SGX is a programming interface for SPs to verify attestation evidence of SGX-enabled enclaves. The API is built using industry-standard Representational State Transfer (REST) architectural style and JavaScript Object Notation (JSON) as the data serialization format.

This specification covers only version 4 of Attestation API.

3.1 Retrieve SigRL

3.1.1 Description

Retrieve the Signature Revocation List (SigRL) for a given EPID group.

SPs are able to retrieve Signature Revocation Lists for EPID groups. EPID SigRLs are generated by Intel and stored in the IAS. They are used to check revocation status of the platform and Quoting Enclave (QE).

Hint: As an optimization, the SP can cache a SigRL retrieved from IAS for a given EPID group and continue to use it until the IAS returns SIGRL_VERSION_MISMATCH for isvEnclaveQuoteStatus in a response to Verify Attestation Evidence. SIGRL_VERSION_MISMATCH indicates that there is a new version of SigRL for a given EPID group that must be used.

3.1.2 API Details

Request		
HTTP method	GET	
HTTP resource	/attestation/v4/sigrl/{gid} *Note: No trailing slash.*	
Request body	N/A	
Request headers	**Header**	**Value**
	Ocp-Apim-Subscription-Key	Subscription Key that provides access to the API (copied as-is from the API portal).
Parameters	{gid} – Base 16-encoded representation of the EPID group ID provided by the platform, encoded as a Big Endian integer.	
Response		
	Status code	**Description**

HTTP status	200 OK	Operation successful.
	401 Unauthorized	Failed to authenticate or authorize request.
	404 Not Found	{gid} does not refer to a valid EPID group ID.
	500 Internal Server Error	Internal error occurred.
	503 Service Unavailable	Service is currently not able to process the request (due to a temporary overloading or maintenance). This is a temporary state – the same request can be repeated after some time.
Response headers	Request-ID	Random generated identifier for each request.
Response body	Base 64-encoded SigRL for EPID group identified by {gid} parameter. If {gid} refers to a valid EPID group but there is no SigRL for this group, then the response body shall be empty and the value of Content-Length response header shall be equal to 0. In any other case (error) the response body will be empty, HTTP status code will define the problem and Request-ID header will be returned to allow further troubleshooting.	

3.1.3 Examples

Note: *The examples below refer only to present sample requests and responses that you might expect from Attestation Service for Intel® SGX in different scenarios. They will not work when used with a real instance of IAS.*

3.1.3.1 SigRL Exists

HTTP request		
URI	GET https://api.trustedservices.intel.com/sgx/attestation/v4/sigrl/00000010	
Headers	Ocp-Apim-Subscription-Key	fe51afe5e0fc488db1e6a7b846692f77
HTTP response		
Status	200 OK	
Headers	Request-ID	de305d5475b4431badb2eb6b9e546014
Body	AAIADgAAAAEAAAABAAAAAGSf/es1h/XiJeCg7bXmX0S/NUpJ2jmcEJglQUI8VT5sLGU7iMFu3/UTCv9uPADal3LhbrQvhBa6+/dWbj8hnsE=	

3.1.3.2 SigRL Does Not Exist

HTTP request	
URI	GET https://api.trustedservices.intel.com/sgx/attestation/v4/sigrl/00000020

Headers	Ocp-Apim-Subscription-Key	fe51afe5e0fc488db1e6a7b846692f77
HTTP response		
Status	200 OK	
Headers	Request-ID	de305d5475b4431badb2eb6b9e546014
Body	<empty>	

3.1.3.3 Invalid EPID Group

HTTP request		
URI	GET https://api.trustedservices.intel.com/sgx/attestation/v4/sigrl/00000030	
Headers	Ocp-Apim-Subscription-Key	fe51afe5e0fc488db1e6a7b846692f77
HTTP response		
Status	404 Not Found	
Headers	Request-ID	de305d5475b4431badb2eb6b9e546014
Body	<empty>	

3.2 Verify Attestation Evidence

3.2.1 Description

Verify submitted attestation evidence and create a new Attestation Verification Report.

The identity of an ISV enclave and the validity of the platform can be verified using Attestation Service for Intel® SGX. The Attestation Service verifies only the validity of the platform. **It is the responsibility of the Service Provider to validate the ISV enclave identity.** As a result of this process, an Attestation Verification Report will be generated and sent back to the SP. The report will include verification results for:

- QUOTE structure generated by the platform for the ISV enclave
- Optional SGX Platform Service Security Property Descriptor provided by the platform.

EPID revocation lists generated by Intel, including EPID Group Revocation Lists (GroupRLs), EPID Private Key Revocation Lists (PrivRLs) and EPID Signature Revocation Lists (SigRLs) will be used to check the revocation status of the platform.

In case the Service Provider registered with a linkable EPID signature policy but uses unlinkable EPID signatures (and vice versa), IAS will respond with "400 Bad Request" to Verify Attestation Evidence call.

Optionally, a signed Platform Info Blob Type-Length-Value (TLV) will be generated and included in the report (as defined in Platform Info Blob section). The SP involved in the remote attestation process should forward Platform Info Blob, excluding the TLV header, to ISV SGX application running on the client platform that is being attested. The ISV SGX application can then process the Platform Info Blob using SGX SDK API sgx_report_attestation_status().

3.2.2 API Details

Request	
HTTP method	POST
HTTP resource	/attestation/v4/report *Note: No trailing slash.*
Request body	Attestation Evidence Payload serialized to JSON: { "isvEnclaveQuote":"<encoded_quote>", "pseManifest":

	"<encoded_SGX_Platform_Service_Security_Property_Descriptor><optional>", "nonce":"<custom_value_passed_by_caller><optional>" }	
Request headers	**Header**	**Value**
	Content-Type	"application/json"
	Ocp-Apim-Subscription-Key	Subscription Key that provides access to the API (copied as-is from the API portal).
Parameters	N/A	
Response		
HTTP status code	**Status code**	**Description**
	200 OK	Operation successful.
	400 Bad Request	Invalid Attestation Evidence Payload. The client should not repeat the request without modifications.
	401 Unauthorized	Failed to authenticate or authorize request.
	500 Internal Server Error	Internal error occurred.
	503 Service Unavailable	Service is currently not able to process the request (due to a temporary overloading or maintenance). This is a temporary state – the same request can be repeated after some time.
Response headers	X-IASReport-Signature	Base 64-encoded Report Signature. This header is present only if HTTP status code is 200.
	X-IASReport-Signing-Certificate	URL encoded Attestation Report Signing Certificate Chain in PEM format (all certificates in the chain, appended to each other). This header is present only if HTTP status code is 200.
	Request-ID	Random generated identifier for each request.
Response body	Attestation Verification Report serialized to a JSON string format: { "id":"<report_id>", "timestamp":"<timestamp>", "version":<version>, "isvEnclaveQuoteStatus":"<quote_status>", "isvEnclaveQuoteBody":"<quote_body>", "revocationReason":<revocation_reason><optional>, "pseManifestStatus":"<pse_manifest_status><optional>", "pseManifestHash":"<pse_manifest_hash><optional>", "platformInfoBlob":"<platform_info_blob><optional>",	

	"nonce":"<custom_value_passed_by_caller><optional>", "epidPseudonym":"<epid_pseudonym_for_linkable><optional>", "advisoryURL":"<advisory_page_URL><optional>", "advisoryIDs":"<array_of_advisory_IDs><optional>" } In case of an error during processing, the response body will be empty (an appropriate HTTP status code will define the problem and Request-ID header returned in case additional troubleshooting actions are required).

3.2.3 Examples

3.2.3.1 Without PSE Manifest

HTTP request		
URI	POST https://api.trustedservices.intel.com/sgx/attestation/v4/report	
Headers	Ocp-Apim-Subscription-Key	fe51afe5e0fc488db1e6a7b846692f77

Body	{
	"isvEnclaveQuote":"AAEAAAEAAA+yth5<...*encoded_quote...*>GuOKBJ+5cs0PQcnZp"
	}	

HTTP response		
Status	200 OK	
Headers	Request-ID	de305d5475b4431badb2eb6b9e546014
	X-IASReport-Signature	lT6EiisC441buJNQhGZwl<...*signature...*>peqiMjar04nQR0AchJkw==
	X-IASReport-Signing-Certificate	-----BEGIN%20CERTIFICATE-----%0AMIIEoT<...*certificate_chain...*> GMnX%0A-----END%20CERTIFICATE-----%0A

Body	{
	"id":"165171271757108173876306223827987629752",
	"timestamp":"2020-03-20T10:07:26.711023",
	"version":4,
	"isvEnclaveQuoteStatus":"OK",
	"isvEnclaveQuoteBody":"AAEAAAEAAA+yth5<...*encoded_quote_body...*>7h38CMfOng"
	}	

3.2.3.2 With PSE Manifest

HTTP request		
URI	POST https://api.trustedservices.intel.com/sgx/attestation/v4/report	
Headers	Ocp-Apim-Subscription-Key	fe51afe5e0fc488db1e6a7b846692f77

Body	{
	"isvEnclaveQuote":"AAEAAAEAAA+yth5<...*encoded_quote...*>GuOKBJ+5cs0PQcnZp",
	"pseManifest":"AAAADsFbEHh9L4RmfOsLW<...*encoded_pse_manifest...*>2cKrl356PqfY3bh+A==
	"
	}

HTTP response		
Status	200 OK	
Headers	Request-ID	de305d5475b4431badb2eb6b9e546014
	X-IASReport-Signature	lT6EiisC441buJNQhGZwl<...*signature...*>peqiMjar04nQR0AchJkw==
	X-IASReport-Signing-Certificate	-----BEGIN%20CERTIFICATE-----%0AMIIEoT<...*certificate_chain...*> GMnX%0A-----END%20CERTIFICATE-----%0A

Body	{
	"id":"165171271757108173876306223827987629752",
	"timestamp":"2020-03-20T10:07:26.711023",
	"version":4,
	"isvEnclaveQuoteStatus":"OK",
	"isvEnclaveQuoteBody":"AAEAAAEAAA+yth5<...*encoded_quote_body...*>7h38CMfOng",
	"pseManifestStatus":"OK",
	"pseManifestHash":"DE75DD331267<...*encoded_pse_manifest_hash...*>4864716FF4B5"
	}	

3.2.3.3 Quote with Linkable EPID Signature

HTTP request		
URI	POST https://api.trustedservices.intel.com/sgx/attestation/v4/report	
Headers	Ocp-Apim-Subscription-Key	fe51afe5e0fc488db1e6a7b846692f77

Body	{
	"isvEnclaveQuote":"AAEAAAEAAA+yth5<...*encoded_quote_with_linkable...*>J+5cs0PQcnZp"
	}	

HTTP response		
Status	200 OK	
Headers	Request-ID	de305d5475b4431badb2eb6b9e546014
	X-IASReport-Signature	lT6EiisC441buJNQhGZwl<...*signature...*>peqiMjar04nQR0AchJkw==
	X-IASReport-Signing-Certificate	-----BEGIN%20CERTIFICATE-----%0AMIIEoT<...*certificate_chain...*> GMnX%0A-----END%20CERTIFICATE-----%0A
Body	{ "id":"165171271757108173876306223827987629752", "timestamp":"2020-03-20T10:07:26.711023",	

	"version":4, "isvEnclaveQuoteStatus":"OK", "isvEnclaveQuoteBody":"AAEAAAEAAA+yth5<...*encoded_quote_body*...>7h38CMfOng", "epidPseudonym":"2p4P9/<...*epid_pseudonym_structure*...>LbGUw8vUEPI/66x8ptZE=" }

3.2.3.4 With Invalid PSE Manifest

HTTP request		
URI	POST https://api.trustedservices.intel.com/sgx/attestation/v4/report	
Headers	Ocp-Apim-Subscription-Key	fe51afe5e0fc488db1e6a7b846692f77

Body	{
	"isvEnclaveQuote":"AAEAAAEAAA+yth5<...*encoded_quote*...>GuOKBJ+5cs0PQcnZp",
	"pseManifest":"AAAADsFbEHh9L4RmfOsLW<...*encoded_invalid_pse_manifest*...>2cKrl356PqfY3bh+A=="
	}	

HTTP response		
Status	200 OK	
Headers	Request-ID	de305d5475b4431badb2eb6b9e546014
	X-IASReport-Signature	lT6EiisC441buJNQhGZwl<...*signature*...>peqiMjar04nQR0AchJkw==
	X-IASReport-Signing-Certificate	-----BEGIN%20CERTIFICATE-----%0AMIIEoT<...*certificate_chain*...>GMnX%0A-----END%20CERTIFICATE-----%0A

Body	{
	"id":"59765165899944768216469568823557519409",
	"timestamp":"2020-03-20T10:13:48.279409",
	"version":4,
	"isvEnclaveQuoteStatus":"OK",
	"isvEnclaveQuoteBody":"AAEAAAEAAA+yth5<...*encoded_quote_body*...>7h38CMfOng",
	"pseManifestStatus":"INVALID",
	"pseManifestHash":"DE75DD331267<...*encoded_pse_manifest_hash*...>4864716FF4B5"
	}	

3.2.3.5 With Nonce

HTTP request		
URI	POST https://api.trustedservices.intel.com/sgx/attestation/v4/report	
Headers	Ocp-Apim-Subscription-Key	fe51afe5e0fc488db1e6a7b846692f77

Body	{
	"isvEnclaveQuote":"AAEAAAEAAAAAAAAADKB5Z<...*encoded_quote*...>AAAAAAAAAAAA==",
	"nonce":"0123456701234567"
	}	

HTTP response		
Status	200 OK	
Headers	Request-ID	de305d5475b4431badb2eb6b9e546014
	X-IASReport-Signature	lT6EiisC441buJNQhGZwl<...*signature...*>peqiMjar04nQR0AchJkw==
	X-IASReport-Signing-Certificate	-----BEGIN%20CERTIFICATE-----%0AMIIEoT<...*certificate_chain...*> GMnX%0A-----END%20CERTIFICATE-----%0A
Body	{ "id":"94974578462868490675968868827087710 68", "timestamp":"2020-03-20T10:07:26.711023", "version":4, "isvEnclaveQuoteStatus":"OK", "isvEnclaveQuoteBody":"AAEAAAEAAA+yth5<...*encoded_quote_body...*>7h38CMfOng", "nonce":"0123456701234567" }	

3.2.3.6 With Invalid Quote

HTTP request		
URI	POST https://api.trustedservices.intel.com/sgx/attestation/v4/report	
Headers	Ocp-Apim-Subscription-Key	fe51afe5e0fc488db1e6a7b846692f77
Body	{ "isvEnclaveQuote":"AAAAADKB5Z<...*encoded_quote...*>AAAAAAAA==" }	

HTTP response		
Status	400 Bad Request	
Headers	Request-ID	de305d5475b4431badb2eb6b9e546014
Body	<empty>	

3.2.3.7 Revoked EPID Group

HTTP request		
URI	POST https://api.trustedservices.intel.com/sgx/attestation/v4/report	
Headers	Ocp-Apim-Subscription-Key	fe51afe5e0fc488db1e6a7b846692f77
Body	{ "isvEnclaveQuote":"AAAAADKB5Z<...*encoded_quote_for_revoked_group ...*>AAAAAAAA==" }	

HTTP response		
Status	200 OK	
Headers	Request-ID	de305d5475b4431badb2eb6b9e546014
	X-IASReport-Signature	lT6EiisC441buJNQhGZwl<...*signature*...>peqiMjar04nQR0AchJkw==
	X-IASReport-Signing-Certificate	-----BEGIN%20CERTIFICATE-----%0AMIIEoT<...*certificate_chain*...> GMnX%0A-----END%20CERTIFICATE-----%0A
Body	{ "id":"664846020604549224883200764779037840 63", "timestamp":"2020-03-20T10:07:26.711023", "version":4, "isvEnclaveQuoteStatus":"GROUP_REVOKED", "isvEnclaveQuoteBody":"AAEAAAEAAA+yth5<...*encoded_quote_body*...>7h38CMfOng", "revocationReason":1, "platformInfoBlob":"150100650<...*pib_structure*...>7B094250DB00C610" }	

3.2.3.8 EPID Group Out Of Date

HTTP request		
URI	POST https://api.trustedservices.intel.com/sgx/attestation/v4/report	
Headers	Ocp-Apim-Subscription-Key	fe51afe5e0fc488db1e6a7b846692f77
Body	{ "isvEnclaveQuote":"AAAAADKB5Z<...*encoded_quote_for_group_out_of_date* ...>AAAAAAAA==" }	
HTTP response		
Status	200 OK	
Headers	Request-ID	de305d5475b4431badb2eb6b9e546014
	X-IASReport-Signature	lT6EiisC441buJNQhGZwl<...*signature*...>peqiMjar04nQR0AchJkw==
	X-IASReport-Signing-Certificate	-----BEGIN%20CERTIFICATE-----%0AMIIEoT<...*certificate_chain*...> GMnX%0A-----END%20CERTIFICATE-----%0A
Body	{ "id":"664846020604549224883200764779037840 63", "timestamp":"2020-03-20T10:07:26.711023", "version":4, "isvEnclaveQuoteStatus":"GROUP_OUT_OF_DATE", "isvEnclaveQuoteBody":"AAEAAAEAAA+yth5<...*encoded_quote_body*...>7h38CMfOng", "platformInfoBlob":"150100650<...*pib_structure*...>7B094250DB00C610",	

	"advisoryURL":"https://security-center.intel.com", "advisoryIDs":["INTEL-SA-00076","INTEL-SA-00135"] }

3.2.3.9 SW Hardening Needed

HTTP request		
URI	POST https://api.trustedservices.intel.com/sgx/attestation/v4/report	
Headers	Ocp-Apim-Subscription-Key	fe51afe5e0fc488db1e6a7b846692f77

Body	{
	"isvEnclaveQuote":"AAAAADKB5Z<...*encoded_quote_for_group_out_of_date*
	...>AAAAAAAA=="
	}	

HTTP response		
Status	200 OK	
Headers	Request-ID	de305d5475b4431badb2eb6b9e546014
	X-IASReport-Signature	lT6EiisC441buJNQhGZwl<...*signature...*>peqiMjar04nQR0AchJkw==
	X-IASReport-Signing-Certificate	-----BEGIN%20CERTIFICATE-----%0AMIIEoT<...*certificate_chain...*> GMnX%0A-----END%20CERTIFICATE-----%0A

Body	{
	"id":"66484602060454922488320076477903784063",
	"timestamp":"2020-03-20T10:07:26.711023",
	"version":4,
	"isvEnclaveQuoteStatus":"SW_HARDENING_NEEDED",
	"isvEnclaveQuoteBody":"AAEAAAEAAA+yth5<...*encoded_quote_body...*>7h38CMfOng",
	"advisoryURL":"https://security-center.intel.com",
	"advisoryIDs":["INTEL-SA-00334"]
	}	

3.2.3.10 Configuration and SW Hardening Needed

HTTP request		
URI	POST https://api.trustedservices.intel.com/sgx/attestation/v4/report	
Headers	Ocp-Apim-Subscription-Key	fe51afe5e0fc488db1e6a7b846692f77

Body	{
	"isvEnclaveQuote":"AAAAADKB5Z<...*encoded_quote_for_group_out_of_date*
	...>AAAAAAAA=="
	}	

HTTP response		
Status	200 OK	
Headers	Request-ID	de305d5475b4431badb2eb6b9e546014
	X-IASReport-Signature	lT6EiisC441buJNQhGZwl<...*signature...*>peqiMjar04nQR0AchJkw==
	X-IASReport-Signing-Certificate	-----BEGIN%20CERTIFICATE-----%0AMIIEoT<*...certificate_chain...*> GMnX%0A-----END%20CERTIFICATE-----%0A
Body	{ "id":"66484602060454922488320076477903784063", "timestamp":"2020-03-20T10:07:26.711023", "version":4, "isvEnclaveQuoteStatus":"CONFIGURATION_AND_SW_HARDENING_NEEDED", "isvEnclaveQuoteBody":"AAEAAAEAAA+yth5<...*encoded_quote_body...*>7h38CMfOng", "platformInfoBlob":"150100650<...*pib_structure*...>7B094250DB00C610", "advisoryURL":"https://security-center.intel.com", "advisoryIDs":["INTEL-SA-00334","INTEL-SA-00161"] }	

4 Data Structures

The following chapter describes in detail the data structures used in the Attestation API.

4.1 Attestation Evidence Payload

Attestation Evidence Payload is a data structure submitted by the Service Provider to IAS so that identity of the ISV enclave and the validity of the platform can be verified.

Data format

Field name	Field type	Field value
isvEnclaveQuote	String	Base 64-encoded QUOTE structure generated by QE for the ISV enclave. See Quoting Data Structures for details. This field is ***mandatory***.
pseManifest	String	Base 64-encoded SGX Platform Service Security Property Descriptor structure provided by the platform. This field is ***optional***, it will be present only if ISV enclave uses SGX Platform Service.
nonce	String	A string that represents custom nonce value provided by SP. Maximum size of the nonce is 32 characters. This field is ***optional***, it is up to the SP to include that field. It can be used by SP to ensure that an old Attestation Verification Report cannot be reused in replay attacks. If this field is present, it will be returned back to SP as part of Attestation Verification Report.

4.2 Attestation Verification Report

The Attestation Verification Report is a data structure returned by the Attestation Service for Intel® SGX to the Service Provider. It contains a cryptographically signed report of verification of the identity of ISV enclave and the Trusted Computing Base (TCB) of the platform.

4.2.1 Report Data

Field name	Field type	Field value
id	String	Representation of unique identifier of the Attestation Verification Report. This field is ***mandatory***.

Field name	Field type	Field value
timestamp	String	Representation of date and time the Attestation Verification Report was created. The time shall be in UTC and the encoding shall be compliant to ISO 8601 standard. This field is ***mandatory***.
version	Number	Integer that denotes the version of the Verification Attestation Evidence API that has been used to generate the report (currently set to 4). Service Providers should verify this field to confirm that the report was generated by the intended API version, instead of a different API version with potentially different security properties. This field is ***mandatory***.
isvEnclaveQuoteStatus	String	One of the following values: • **OK** – EPID signature of the ISV enclave QUOTE was verified correctly and the TCB level of the SGX platform is up-to-date. • **SIGNATURE_INVALID** – EPID signature of the ISV enclave QUOTE was invalid. The content of the QUOTE is not trustworthy. • **GROUP_REVOKED** – The EPID group has been revoked. When this value is returned, the revocationReason field of the Attestation Verification Report will contain revocation reason code for this EPID group as reported in the EPID Group CRL. The content of the QUOTE is not trustworthy. • **SIGNATURE_REVOKED** – The EPID private key used to sign the QUOTE has been revoked by signature. The content of the QUOTE is not trustworthy. • **KEY_REVOKED** – The EPID private key used to sign the QUOTE has been directly revoked (not by signature). The content of the QUOTE is not trustworthy. • **SIGRL_VERSION_MISMATCH** – SigRL version in ISV enclave QUOTE does not match the most recent version of the SigRL. In rare situations, after SP retrieved the SigRL from IAS and provided it to the platform, a newer version of the SigRL is made available. As a result, the Attestation Verification Report will indicate SIGRL_VERSION_MISMATCH. SP can retrieve the most recent version of SigRL from the IAS and request the platform to perform remote attestation again with the most recent version of SigRL. If the platform keeps failing to provide a valid QUOTE matching with the most recent version of the SigRL, the content of the QUOTE is not trustworthy. • **GROUP_OUT_OF_DATE** – The EPID signature of the ISV enclave QUOTE has been verified correctly, but the

Field name	Field type	Field value
		TCB level of SGX platform is outdated (for further details see Advisory IDs). The platform has not been identified as compromised and thus it is not revoked. It is up to the Service Provider to decide whether or not to trust the content of the QUOTE, and whether or not to trust the platform performing the attestation to protect specific sensitive information. • **CONFIGURATION_NEEDED** - The EPID signature of the ISV enclave QUOTE has been verified correctly, but additional configuration of SGX platform may be needed (for further details see Advisory IDs). The platform has not been identified as compromised and thus it is not revoked. It is up to the Service Provider to decide whether or not to trust the content of the QUOTE, and whether or not to trust the platform performing the attestation to protect specific sensitive information. • **SW_HARDENING_NEEDED** – the EPID signature of the ISV enclave QUOTE has been verified correctly but due to certain issues affecting the platform, additional SW Hardening in the attesting SGX enclaves may be needed. The relying party should evaluate the potential risk of an attack leveraging the relevant issues on the attesting enclave, and whether the attesting enclave employs adequate software hardening to mitigate the risk. • **CONFIGURATION_AND_SW_HARDENING_NEEDED** – the EPID signature of the ISV enclave QUOTE has been verified correctly but additional configuration for the platform and SW Hardening in the attesting SGX enclaves may be needed. The platform has not been identified as compromised and thus it is not revoked. It is up to the Service Provider to decide whether or not to trust the content of the QUOTE. The relying party should also evaluate the potential risk of an attack leveraging the relevant issues on the attestation enclave, and whether the attesting enclave employs adequate software hardening to mitigate the risk. This field is ***mandatory***.
isvEnclaveQuoteBody	String	Base 64-encoded BODY of QUOTE structure (i.e., QUOTE structure without signature related fields: SIG_LEN and SIG) as received in Attestation Evidence Payload. See Quoting Data Structures for details. This field is ***mandatory***.

Field name	Field type	Field value
revocationReason	Number	Integer corresponding to revocation reason code for a revoked EPID group listed in EPID Group CRL. Allowed values are described in RFC 5280. This field is ***optional***, it will only be present if value of isvEnclaveQuoteStatus is equal to GROUP_REVOKED.
pseManifestStatus	String	One of the following values: • **OK** – Security properties of the SGX Platform Service was verified as valid and up-to-date. • **UNKNOWN** – Security properties of the SGX Platform Service cannot be verified due to unrecognized PSE Manifest. • **INVALID** – Security properties of the SGX Platform Service are invalid. SP should assume the SGX Platform Service utilized by the ISV enclave is invalid. • **OUT_OF_DATE** – TCB level of SGX Platform Service is outdated but the Service has not been identified as compromised and thus it is not revoked. It is up to the SP to decide whether or not to assume the SGX Platform Service utilized by the ISV enclave is valid. • **REVOKED** – The hardware/firmware component involved in the SGX Platform Service has been revoked. SP should assume the SGX Platform Service utilized by the ISV enclave is invalid. • **RL_VERSION_MISMATCH** – A specific type of Revocation List used to verify the hardware/firmware component involved in the SGX Platform Service during the SGX Platform Service initialization process is out of date. If the SP rejects the remote attestation and forwards the Platform Info Blob to the SGX Platform SW through the ISV SGX Application, the SGX Platform SW will attempt to refresh the SGX Platform Service. This field is ***optional***, it will only be present if the SGX Platform Service Security Property Descriptor (pseManifest) is provided in Attestation Evidence Payload and isvEnclaveQuoteStatus is equal to OK, GROUP_OUT_OF_DATE, CONFIGURATION_NEEDED, SW_HARDENING_NEEDED or CONFIGURATION_AND_SW_HARDENING_NEEDED.
pseManifestHash	String	SHA-256 calculated over SGX Platform Service Security Property Descriptor as received in Attestation Evidence Payload. This field is encoded using Base 16 encoding scheme.

Field name	Field type	Field value
		This field is ***optional***, it will only be present if pseManifest field is provided in Attestation Evidence Payload.
platformInfoBlob	String	A TLV containing an opaque binary blob that the Service Provider and the ISV SGX Application are supposed to forward to SGX Platform SW. This field is encoded using Base 16 encoding scheme. This field is ***optional***, it will only be present if one the following conditions is met: • isvEnclaveQuoteStatus is equal to GROUP_REVOKED, GROUP_OUT_OF_DATE, CONFIGURATION_NEEDED or CONFIGURATION_AND_SW_HARDENING_NEEDED. • pseManifestStatus is equal to one of the following values: OUT_OF_DATE, REVOKED or RL_VERSION_MISMATCH.
nonce	String	A string that represents a nonce value provided by SP in Attestation Evidence Payload. This field is ***optional***, it will only be present if nonce field is provided in Attestation Evidence Payload.
epidPseudonym	String	Byte array representing EPID Pseudonym that consists of the concatenation of EPID B (64 bytes) & EPID K (64 bytes) components of EPID signature. If two linkable EPID signatures for an EPID Group have the same EPID Pseudonym, the two signatures were generated using the same EPID private key. This field is encoded using Base 64 encoding scheme. This field is ***optional***, it will only be present if Attestation Evidence Payload contains Quote with *linkable* EPID signature.
advisoryURL	String	URL to Intel® Product Security Center Advisories page that provides additional information on SGX-related security issues. IDs of advisories for specific issues that may affect the attested platform are conveyed in advisoryIDs field. This field is ***optional***, it will only be present if HTTP status code is 200 and isvEnclaveQuoteStatus in Attestation Verification Report is equal to GROUP_OUT_OF_DATE, CONFIGURATION_NEEDED, SW_HARDENING_NEEDED or CONFIGURATION_AND_SW_HARDENING_NEEDED.
advisoryIDs	Array	JSON array of Advisory IDs (e.g. [“INTEL-SA-00075“,“INTEL-SA-00076”]) that can be searched on a page indicated by URL included in advisoryURL field. Advisory IDs refer to articles providing insight into SGX-related security issues that may affect attested platform.

Field name	Field type	Field value
		This field is ***optional***, it will only be present if HTTP status code is 200 and isvEnclaveQuoteStatus in Attestation Verification Report is equal to GROUP_OUT_OF_DATE, CONFIGURATION_NEEDED, SW_HARDENING_NEEDED or CONFIGURATION_AND_SW_HARDENING_NEEDED.

4.2.2 Report Signature

The Attestation Verification Report is cryptographically signed by Report Signing Key (owned by the Attestation Service) using the RSA-SHA256 algorithm. The signature is calculated over the entire body of the HTTP response. Base 64-encoded signature is then returned in a custom HTTP response header X-IASReport-Signature.

To verify the signature over the report, you should the following steps:

1. Decode and verify the Report Signing Certificate Chain that was sent together with the report (see Report Signing Certificate Chain for details). Verify that the chain is rooted in a trusted Attestation Report Signing CA Certificate (available to download upon successful registration to IAS).
2. Optionally, verify that the certificates in the chain have not been revoked (using CRLs indicated in the certificates).
3. Verify the signature over the report using Attestation Report Signing Certificate.

4.2.3 Report Signing Certificate Chain

The public part of Report Key is distributed in the form of an x.509 digital certificate called Attestation Report Signing Certificate. It is a leaf certificate issued by the Attestation Report Signing CA Certificate:

1) **Attestation Report Signing CA Certificate:** CN=Intel SGX Attestation Report Signing CA, O=Intel Corporation, L=Santa Clara, ST=CA, C=US
2) **Attestation Report Signing Certificate:** CN=Intel SGX Attestation Report Signing, O=Intel Corporation, L=Santa Clara, ST=CA, C=US

A PEM-encoded certificate chain consisting of Attestation Report Signing Certificate and Attestation Report Signing CA Certificate is returned in a custom HTTP response header X-IASReport-Signing-Certificate.

4.2.4 Platform Info Blob

Platform Info Blob TLV contains an opaque data structure to be forwarded from the Service Provider to the ISV SGX application. The ISV SGX application can then call the SGX SDK API sgx_report_attestation_status () for analysis. Internally, the *Platform Info Blob TLV* is a collection of status flags and platform TCB information wrapped in a TLV container (that includes a header). All *TLV header* ingredients are expressed in big-endian.

4.2.4.1 Platform Info Blob TLV

Name		Size (Bytes)	Description
TLV Header	Type	1	Identifier of Platform Info Blob TLV (*value: 21*).
	Version	1	Version of the data structure (*value: 2*).
	Size	2	The size of TLV Payload data that follows this field.
TLV Payload	Platform Info Blob	Variable	Platform Information Blob to be processed by SGX Platform SW.

4.3 Quoting Data Structures

4.3.1 QUOTE Structure

Name		Offset (Bytes)	Size (Bytes)	Description
BODY	VERSION	0	2	Version of this structure. (Little-endian integer) • Value: 2
	SIGNATURE_TYPE	2	2	Type of the signature. Bit 0: 0 – unlinkable 1 – linkable Other bits reserved.
	GID	4	4	ID of platform's EPID Group. (Little-endian integer)
	ISVSVN_QE	8	2	The security version of the QE. (Little-endian integer)
	ISVSVN_PCE	10	2	The security version of the PCE. (Little-endian integer) This field is filled only in case of QUOTE with VERSION set to 2. In case of QUOTE with VERSION set to 1, it is 0'ed.
	RESERVED	12	4	Reserved bytes (set to 0).
	BASENAME	16	32	EPID basename used in Quote.
REPORTBODY	CPUSVN	48	16	The security version of the CPU represented as a byte array.
	MISCSELECT	64	4	SSA frame extended feature set for the enclave. (Little-endian integer)
	RESERVED	68	28	Reserved bytes (set to 0).

Name		Offset (Bytes)	Size (Bytes)	Description
	ATTRIBUTES	96	16	The values of the attributes flags for the enclave.
	MRENCLAVE	112	32	Enclave measurement represented as SHA256 digest (as defined in FIPS PUB 180-4).
	RESERVED	144	32	Reserved bytes (set to 0).
	MRSIGNER	176	32	SHA256 digest (as defined in FIPS PUB 180-4) of the big endian format modulus of the RSA public key of the enclave's signing key pair.
	RESERVED	208	96	Reserved bytes (set to 0).
	ISVPRODID	304	2	Enclave Product ID. (Little-endian integer)
	ISVSVN	306	2	The security version of the enclave. (Little-endian integer)
	RESERVED	308	60	Reserved bytes (set to 0).
	REPORTDATA	368	64	The value of REPORT.ReportData in REPORT input of GetQuote() or UserData in NB_UD input of GetQuote().
SIG_LEN		432	4	Length of SIG field in bytes. SIG_LEN is not part of the data the signature is based on. (Little-endian integer)
SIG		436	variable	Encrypted EPID signature over BODY and REPORTBODY.

4.4 SGX Platform Service Security Property Descriptor

SGX Platform Service Security Property Descriptor is an opaque 256 byte data structure provided by the platform.