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

Intel® Software Guard Extensions (Intel® SGX)认证服务:API 文档

Revision: 4.1

翻译整理 By 魔力派
2019-4-11

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).

Intel®SGX 认证服务(IAS)是由 Intel 在云环境中托管和运营的 Web 服务。IAS 的主要职责是验证服务提供商(SP)提交的认证证据。

2.1. Supported Environments

Development Environment *– test environment established for software development purposes (early developer integration):*

开发环境 — 为软件开发目的而建立的测试环境(早期开发人员集成):

https://test-as.sgx.trustedservices.intel.com:443

Production Environment *– production-quality environment to be used by production ready software:*

生产环境 — 产品级质量环境，用于生产就绪软件:

https://as.sgx.trustedservices.intel.com:443

2.2. Authentication

Attestation Service for Intel® SGX uses MTLS (Mutual Transport Layer Security) as an authentication mechanism. This means that both server and client must introduce themselves with valid certificates, both signed by a trusted certificate authority. The client's certificate must be registered in IAS as part of the Service Provider registration. Refer to Section 2.4 in this document for more information.

英特尔®SGX 认证服务使用 MTLS(互传输层安全)作为认证机制。这意味着服务器和客户机都必须使用由受信任的证书颁发机构签名的有效证书来介绍自己。客户端证书必须作为服务提供者注册流程的一部分在 IAS 中注册。有关更多信息，请参阅本文档的第 2.4 节。

2.2.1. Supported TLS Versions

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

英特尔®SGX 认证服务只接受被 TLS 1.2 或更高版本保护的连接。IAS 将丢弃使用 SSL 协议任何版本的任何传入连接。

2.3. Available API Versions

The latest available API version exposed by Attestation Service for Intel® SGX is version 3. **Attestation API version 2 is considered deprecated and is on the path to End of Life (EOL).** This document focuses only on API version 3, for API version 2 refer to the previous revision of IAS API specification.

英特尔®SGX 认证服务公开的最新可用 API 版本是版本 3。认证 API 版本 2 被认为是不受支持的，并且正在走向生命终结(EOL)。本文档只关注 API 版本 3，因为 API 版本 2 参考了 IAS API 规范的上一版本。

2.3.1. Summary of API v3 Changes

The changes introduced in Attestation API version 3 are mainly focused in the following areas:

1) Verify Attestation Evidence API has been updated, specifically a new status (CONFIGURATION_NEEDED) has been added to isvEnclaveQuoteStatus in Attestation Verification Report (see Section Section 4.2.1 for further details).
2) Version field has been added to Attestation Verification Report reflecting the version of the API that has been used to generate the report (see Section Section 4.2.1 for further details).
3) Security Advisory IDs have been introduced and they are now returned along with Attestation Verification Report. The Advisory IDs can be looked up on Intel® Product Security Center Advisories page (https://security-center.intel.com) in order to get additional information on SGX related security issues that affect attested platforms (see Section 3.2.2 for further details).

认证 API 第三版引入的变化主要集中在以下几个方面:

1) 验证认证证据 API 已更新，特别是在验证报告 isvEnclaveQuoteStatus 中添加了一个新的状态(configuration_required)(详见 4.2.1 节)。
2) 已在认证验证报告中添加版本字段，反映生成报告所用 API 的版本(详见 4.2.1 节)。
3) 引入了安全咨询 ID，现在连同认证验证报告一起返还。咨询 ID 可以在 Intel®产品安全中心顾问页面(https://securcenter.intel.com)上查询，以获得有关影响认证平台的 SGX 相关安全问题的额外信息(详细信息请参见第 3.2.2 节)。

2.4. Registering for the Service

Registration of Service Providers (SPs) will be handled via the request form linked from http://software.intel.com/sgx. As part of this process, the following artifacts must be delivered by SPs:
服务提供者(SP)的注册将通过链接 http://software.intel.com/sgx 的请求表单来处理。作为此过程的一部分，以下构件必须由 SP 交付:

- ***X.509 client certificate*** that identifies the SP. This certificate will be registered in IAS and used by the SP to authenticate to the service. As a result IAS will be configured to support only registered SPs. The certificate needs to be issued by a commonly trusted Certificate Authority (CA) (e.g., Verisign) to be registered in the Production Environment. The Development Services Environment does not have that restriction - a valid self-signed certificate can be used. Details on client certificate requirements for IAS are available at the following link:
  https://software.intel.com/en-us/articles/certificate-requirements-for-intel-attestation-services.
  X.509 客户端证书，用于识别 SP。该证书将在 IAS 中注册，SP 将使用该证书对服务进行身份验证。因此，IAS 将配置为仅支持已注册的 SP。证书需要由普遍受信任的证书颁发机构（CA）（例如，Verisign）颁发，以在生产环境中注册。开发服务环境没有这种限制——可以使用有效的自签名证书。有关 IAS 客户端证书要求的详情，请浏览以下连结: https://software.intel.com/en-us/articles/certificate-requirements-for-intel-attestation-services。

- ***Email address(es)*** that will be used to notify the Service Provider about updates and availability of IAS (e.g. planned and unplanned downtimes, limited availability alerts) as well as revocation data updates. In some 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 (e.g. engineering, operations, etc.).
  电子邮件地址，用于通知服务提供商有关 IAS 的更新和可用性（例如计划内和计划外停机时间，可用性限制警报）以及吊销数据更新。在某些情况下，提供的电子邮件地址是可公开寻址的企业分发列表，以便企业可以管理谁接收通知(例如工程、操作等)，这可能是有益的。
- ***Linkable/Unlinkable EPID signatures policy setting*** that determines if the Service Provider wants to use Linkable or Unlinkable EPID signatures in enclave quotes.
  可链接/不可链接 EPID 签名策略设置，确定服务提供者是否希望在 enclave quotes 中使用可链接或不可链接的 EPID 签名。

2.5. Troubleshooting

Each HTTP call to the API will result 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.
对 API 的每个 HTTP 调用都会产生一个响应，其中包含一个名为 Request-ID 的头部。Request-ID 的值包含一个随机生成的通用惟一标识符(UUID)，可用于跟踪单个 HTTP 请求。如果出现错误，SP 应该记录这个头的值，并将其包含在问题提交中，以便进行进一步的故障排除。

3. Attestation API (version 3)

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.
Intel®SGX 认证服务公开的认证 API 是一个用于 SP 的编程接口，用于验证启用 SGX 的 enclaves 的认证证据。该 API 使用行业标准的 Representational State Transfer（REST）架构风格和 JavaScript Object Notation（JSON）作为数据序列化格式构建。

This specification covers only version 3 of Attestation API (**version 2** is considered **deprecated**).
此规范仅涵盖认证 API 的版本 3（版本 2 被视为已弃用）。

3.1. Retrieve SigRL

3.1.1. Description

Retrieve the Signature Revocation List (SigRL) for a given EPID group.
检索给定 EPID 组的签名撤销列表(SigRL)。

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).
SP 能够检索 EPID 组的签名撤销列表。EPID SigRLs 由 Intel 生成并存储在 IAS 中。它们用于检查平台和 Quoting Enclave (QE) 的撤销状态。

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.
提示：作为优化，SP 可以缓存从 IAS 为给定 EPID 组检索的 SigRL，并继续使用它，直到 IAS 在验证认证证据的响应中返回 isvEnclaveQuoteStatus 的 SIGRL_VERSION_MISMATCH。
SIGRL_VERSION_MISMATCH 表示必须使用给定 EPID 组的 SigRL 的新版本。

3.1.2. API Details

Request /请求		
HTTP method	GET	
HTTP resource	/attestation/sgx/v3/sigrl/{gid} *Note: No trailing slash.* *注意：没有末尾斜杠.*	
Request body	N/A	
Request headers	N/A	
Parameters	{gid} – Base 16-encoded representation of the EPID group ID provided by the platform, encoded as a Big Endian integer. {gid} - 由平台提供的 EPID 组 ID 的 Base 16 编码表示，编码为 Big Endian 整数。	
Response /响应		
HTTP status	**Status code**	**Description**
	200 OK	Operation successful. 操作成功。
	401 Unauthorized	Failed to authenticate or authorize request. 验证或授权请求失败。
	404 Not Found	{gid} does not refer to a valid EPID group ID. {gid}没有引用有效的 EPID 组 ID。
	500 Internal Server Error	Internal error occurred. 发生内部错误。

	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. 服务目前无法处理请求(由于临时超载或维护)。这是一个临时状态——相同的请求可以在一段时间后重发。
Response headers	Request-ID	Random generated identifier for each request. 为每个请求随机生成的标识符。
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. 由{gid}参数标识的 EPID 组的 Base64 编码的签名撤销列表(SigRL)。如果{gid}引用一个有效的 EPID 组，但是这个组没有 SigRL，那么响应体应该是空的，Content-Length 响应头的值应该等于 0。在任何其他情况下(错误)，响应体将为空，HTTP 状态代码将定义问题，并返回 Request-ID 头，以便进行进一步的故障排除。	

3.1.3. Examples

Note: The examples below are 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.

注意：以下示例仅用于介绍在不同情况下您可能从英特尔®SGX 的认证服务中获得的示例请求和响应。 当与 IAS 的实际实例一起使用时，它们将无法工作。

3.1.3.1 SigRL Exists

HTTP request		
URI	GET https://test-as.sgx.trustedservices.intel.com:443/attestation/sgx/v3/sigrl/00000010	
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://test-as.sgx.trustedservices.intel.com:443/attestation/sgx/v3/sigrl/00000020
HTTP response	

Status	200 OK	
Headers	Request-ID	de305d5475b4431badb2eb6b9e546014
Body	<empty>	

3.1.3.3 Invalid EPID Group

HTTP request		
URI	GET https://test-as.sgx.trustedservices.intel.com:443/attestation/sgx/v3/sigrl/00000030	
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.
验证提交的认证证据，并创建新的认证验证报告。

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

可以使用 Intel®SGX 的认证服务来验证 ISV enclave 的身份和平台的有效性。认证服务只验证平台的有效性。**验证 ISV enclave 标识是服务提供者的责任。**在此过程中，将生成一份认证验证报告并发回给 SP。该报告将包括对以下内容的验证结果：

- ISV enclave 平台生成的 QUOTE 结构
- 可选的平台提供的 SGX 平台服务安全属性描述符(SGX Platform Service Security Property Descriptor)

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.
使用 Intel 生成的 EPID 撤销列表来检查平台的撤销状态，包括 EPID 组撤销列表(GroupRLs)、EPID 私钥撤销列表(PrivRLs)和 EPID 签名撤销列表(SigRLs)。

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.
如果服务提供者注册了可链接的 EPID 签名策略，但使用了不可链接的 EPID 签名(反之亦然)，则 IAS 将向验证认证证据调用响应“400 Bad Request”。

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().
（可选）还可以生成一个带签名的 Type-Length-Value (TLV)格式的平台信息块(Platform Info Blob)，并将其包含在报告中(如平台信息块(Platform Info Blob)部分中所定义)。远程认证过程中涉及的 SP 应该将平台信息块 (TLV 头除外)转发到正在被认证的客户机平台上运行的 ISV SGX 应用程序。然后 ISV SGX 应用程序可以使用 SGX SDK API: sgx_report_attestation_status()处理平台信息块。

3.2.2. API Details

Request /请求

HTTP method	POST	
HTTP resource	/attestation/sgx/v3/report *Note: No trailing slash.* *注意：没有末尾斜杠.*	

Request body	Attestation Evidence Payload serialized to JSON:
	认证证据有效负载序列化为 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”
Parameters	N/A	
Response /响应		
HTTP status code	**Status code**	**Description**
	200 OK	Operation successful. 操作成功。
	400 Bad Request	Invalid Attestation Evidence Payload. The client should not repeat the request without modifications. 无效的认证证据有效负载。客户端不应该在没有修改的情况下重复请求。
	401 Unauthorized	Failed to authenticate or authorize request. 验证或授权请求失败。
	500 Internal Server Error	Internal error occurred. 发生内部错误。
	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. 服务目前无法处理请求(由于临时超载或维护)。这是一个临时状态——相同的请求可以在一段时间后重发。
Response headers	X-IASReport-Signature	Base 64-encoded Report Signature. This header is present only if HTTP status code is 200. Base64 编码的报告签名。 仅当 HTTP 状态码为 200 时才有此字段。

	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. 以PEM格式编码的URL认证报告签名证书链(链中的所有证书，相互附加)。 仅当HTTP状态码为200时才有此字段。
	Advisory-URL	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 Advisory IDs header. This header is present only if HTTP status code is 200 and isvEnclaveQuoteStatus in Attestation Verification Report is equal to GROUP_OUT_OF_DATE or CONFIGURATION_NEEDED. “英特尔®产品安全中心公告”页面的URL，提供有关SGX相关安全问题的额外信息。对于可能影响已验证平台的特定问题，其公告ID将在公告ID头中传达。 仅当HTTP状态代码为200且在认证验证报告中为isvEnclaveQuoteStatus等于GROUP_OUT_OF_DATE或CONFIGURATION_NEEDED时，此字段才会出现。
	Advisory-IDs	Comma-separated list of Advisory IDs (e.g. “INTEL-SA00075, INTEL-SA-00076”) that can be searched on a page indicated by URL included in Advisory-URL header. Advisory IDs refer to articles providing insight into SGXrelated security issues that may affect attested platform. This header is present only if HTTP status code is 200 and isvEnclaveQuoteStatus in Attestation Verification Report is equal to GROUP_OUT_OF_DATE or CONFIGURATION_NEEDED. 以逗号分隔的公告ID列表（例如“INTEL-SA00075，INTEL-SA-00076”），可以在Advisory-URL头中包含的URL指示的页面上搜索。 公告ID指向提供对可能影响认证平台的SGX相关安全问题的深入了解的文章。 仅当HTTP状态代码为200且证明验证报告中的isvEnclaveQuoteStatus等于GROUP_OUT_OF_DATE或CONFIGURATION_NEEDED时，此字段才会出现。
	Request-ID	Random generated identifier for each request. 为每个请求随机生成的标识符。
Response body	Attestation Verification Report serialized to a JSON string format: 认证验证报告序列化为JSON字符串格式: { "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>" } 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). 如果在处理过程中出现错误，响应正文将为空(适当的 HTTP 状态代码将定义问题，并在需要额外的故障排除操作时返回 Request-ID 头)。

3.2.3. Examples

3.2.3.1 Without PSE Manifest

HTTP request		
URI	POST https://test-as.sgx.trustedservices.intel.com:443/attestation/sgx/v3/report	

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-SigningCertificate	-----BEGIN%20CERTIFICATE-----%0AMIIEoT<*...certificate_chain...*> GMnX%0A-----END%20CERTIFICATE-----%0A

Body	{
	"id":"165171271757108173876306223827987629752",
	"timestamp":"2015-09-29T10:07:26.711023",
	"version":3,
	"isvEnclaveQuoteStatus":"OK",
	"isvEnclaveQuoteBody":"AAEAAAEAAA+yth5<*…encoded_quote_body…*>7h38CMfOng"
	}	

3.2.3.2 With PSE Manifest

HTTP request		
URI	POST https://test-as.sgx.trustedservices.intel.com:443/attestation/sgx/v3/report	

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-SigningCertificate	-----BEGIN%20CERTIFICATE-----%0AMIIEoT<...*certificate_chain*...> GMnX%0A-----END%20CERTIFICATE-----%0A

Body	{
	"id":"165171271757108173876306223827987629752",
	"timestamp":"2015-09-29T10:07:26.711023",
	"version":3,
	"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://test-as.sgx.trustedservices.intel.com:443/attestation/sgx/v3/report	

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-SigningCertificate	-----BEGIN%20CERTIFICATE-----%0AMIIEoT<...*certificate_chain...*> GMnX%0A-----END%20CERTIFICATE-----%0A

Body	{
	"id":"165171271757108173876306223827987629752",
	"timestamp":"2015-09-29T10:07:26.711023",
	"version":3,
	"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://test-as.sgx.trustedservices.intel.com:443/attestation/sgx/v3/report	

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-SigningCertificate	-----BEGIN%20CERTIFICATE-----%0AMIIEoT<...*certificate_chain...*> GMnX%0A-----END%20CERTIFICATE-----%0A

Body	{
	"id":"59765165899944768216469568823557519409",
	"timestamp":"2015-09-29T10:13:48.279409",
	"version":3,
	"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://test-as.sgx.trustedservices.intel.com:443/attestation/sgx/v3/report	

Body	{
	"isvEnclaveQuote":"AAEAAAEAAAAAAAADKB5Z<*…encoded_quote…*>AAAAAAAAAAAA==",
	"nonce":"0123456701234567"
	}	

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

Body	{
	"id":"9497457846286849067596886882708771068",
	"timestamp":"2015-09-29T10:07:26.711023",
	"version":3,
	"isvEnclaveQuoteStatus":"OK",
	"isvEnclaveQuoteBody":"AAEAAAEAAA+yth5<*…encoded_quote_body…*>7h38CMfOng",
	"nonce":"0123456701234567"
	}	

3.2.3.6 With Invalid Quote

HTTP request		
URI	POST https://test-as.sgx.trustedservices.intel.com:443/attestation/sgx/v3/report	

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://test-as.sgx.trustedservices.intel.com:443/attestation/sgx/v3/report	

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-SigningCertificate	-----BEGIN%20CERTIFICATE-----%0AMIIEoT<*...certificate_chain...*> GMnX%0A-----END%20CERTIFICATE-----%0A

Body	{
	"id":"66484602060454922488320076477903784063",
	"timestamp":"2015-09-29T10:07:26.711023",
	"version":3,
	"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://test-as.sgx.trustedservices.intel.com:443/attestation/sgx/v3/report	

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-SigningCertificate	-----BEGIN%20CERTIFICATE-----%0AMIIEoT<*...certificate_chain...*> GMnX%0A-----END%20CERTIFICATE-----%0A
	Advisory-URL	https://security-center.intel.com

	Advisory-IDs	INTEL-SA-00076,INTEL-SA-00135

Body	{
	"id":"66484602060454922488320076477903784063",
	"timestamp":"2015-09-29T10:07:26.711023",
	"version":3,
	"isvEnclaveQuoteStatus":"GROUP_OUT_OF_DATE",
	"isvEnclaveQuoteBody":"AAEAAAEAAA+yth5<…*encoded_quote_body…*>7h38CMfOng",
	"platformInfoBlob":"150100650<…*pib_structure*…>7B094250DB00C610"
	}	

4. Data Structures

The following chapter describes in detail the data structures used in the Attestation API.
下述章节将详细描述认证 API 中用到的数据结构。

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.
认证证据有效负载是服务提供者向 IAS 提交的数据结构，以便验证 ISV enclave 的身份和平台的有效性。

Data format / 数据格式

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. 由 QE(Quoting Enclave)为 ISV enclave 生成的 Base64 编码的 QUOTE 结构。有关详细信息，请参见 Quoting Data Structures。 This field is ***mandatory***. 这个字段是强制性的。
pseManifest	String	Base 64-encoded SGX Platform Service Security Property Descriptor structure provided by the platform. 由平台提供的 Base64 编码的 SGX 平台服务安全属性描述符结构。 This field is ***optional***, it will be present only if ISV enclave uses SGX Platform Service. 这个字段是可选的，只有 ISV enclave 使用 SGX 平台服务时才会出现。
nonce	String	A string that represents custom nonce value provided by SP. Maximum size of the nonce is 32 characters. 表示 SP 提供的自定义 nonce 值的字符串。nonce 最大为 32 个字符。 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. 该字段是可选的，由 SP 决定是否包含该字段。SP 可以使用它来确保旧的认证验证报告不能在重放攻击中重用。 If this field is present, it will be returned back to SP as part of Attestation Verification Report. 如果该字段存在，它将作为认证验证报告的一部分返回给 SP。

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.
认证验证报告是英特尔®SGX 认证服务返回给服务提供商的数据结构。它包含一个对 ISV enclave 身份和平台可信计算基(TCB)的密码学签名的验证报告。

4.2.1. Report Data

Field name	Field type	Field value
id	String	Representation of unique identifier of the Attestation Verification Report. 表示认证验证报告的唯一标识符。 This field is ***mandatory***. 这个字段是强制性的。
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. 表示创建认证验证报告的日期和时间。应为 UTC 时间且编码符合 ISO 8601 标准。 This field is ***mandatory***. 这个字段是强制性的。
version	Number	Integer that denotes the version of the Verification Attestation Evidence API that has been used to generate the report (currently set to 3). 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. 整数表示的验证认证证据 API 版本，用于生成报告(目前设置为 3)。服务提供商应该验证这个字段以确认报告是用期望的 API 版本生成的，因为不同的 API 版本可能有不同的安全属性。 This field is ***mandatory***. 这个字段是强制性的。
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. ISV enclave QUOTE 的 EPID 签名验证正确，并且 SGX 平台的 TCB 级别是最新的。 • **SIGNATURE_INVALID** – EPID signature of the ISV enclave QUOTE was invalid. The content of the QUOTE is not trustworthy. ISV enclave QUOTE 的 EPID 签名无效。QUOTE 的内容不可信。

		• **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. 该 EPID 组已被撤消。当返回此值时，认证验证报告的 revocationReason 字段将包含 EPID 组 CRL 中所报告的此 EPID 组的吊销原因代码。QUOTE 的内容不可信。 • **SIGNATURE_REVOKED** – The EPID private key used to sign the QUOTE has been revoked by signature. The content of the QUOTE is not trustworthy. 用于签署 QUOTE 的 EPID 私钥已被签名撤销。 QUOTE 的内容不可信。 • **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. 用于签署 QUOTE 的 EPID 私钥已被直接撤销（不是通过签名）。 QUOTE 的内容不可信。 • **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. ISV enclave QUOTE 中的 SigRL 版本跟 SigRL 的最新版本不匹配。在极少数情况下，SP 从 IAS 检索 SigRL 并将其提供给平台之后，就可以使用 SigRL 的新版本。因此，认证验证报告将指示 SIGRL_VERSION_MISMATCH。SP 可以从 IAS 中检索最新版本的 SigRL，并请求平台再次使用最新版本的 SigRL 进行远程认证。如果平台始终无法提供与 SigRL 最新版本匹配的有效 QUOTE，那么 QUOTE 的内容就不可信。 • **GROUP_OUT_OF_DATE** – The EPID signature of the ISV enclave QUOTE has been verified correctly, but the 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. ISV enclave QUOTE 的 EPID 签名已被正确验证，但 SGX 平台的 TCB 级别已经过时(更多细节请参见咨询 ID)。该平台尚未被确定为受危害的，因此没有被撤销。由服务提供

		商决定是否信任 QUOTE 的内容，以及是否信任执行认证的平台以保护特定敏感信息。 • **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. ISV enclave QUOTE 的 EPID 签名已被正确验证，但 SGX 平台可能需要额外的配置(更多细节请参见咨询 ID)。该平台尚未被确定为受危害的，因此没有被撤销。由服务提供商决定是否信任 QUOTE 的内容，以及是否信任执行认证的平台以保护特定敏感信息。 This field is ***mandatory***. 这个字段是强制性的。
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. 在认证证据有效载荷中接收的 Base64 编码的 QUOTE 结构的 BODY(即， QUOTE 结构没有签名相关字段: SIG_LEN 和 SIG)。 有关详细信息， 请参阅 Quoting Data Structures。 This field is ***mandatory***. 这个字段是强制性的。
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. 对应于 EPID 组 CRL 中列出的已撤销 EPID 组的撤销原因代码的整数。允许的值在 RFC 5280 中描述。 This field is ***optional***, it will only be present if value of isvEnclaveQuoteStatus is equal to GROUP_REVOKED. 此字段是可选的，仅当 isvEnclaveQuoteStatus 的值等于 GROUP_REVOKED 时才会出现。
pseManifestStatus	String	One of the following values: • **OK** – Security properties of the SGX Platform Service was verified as valid and up-to-date. SGX 平台服务的安全属性被验证为有效且最新的。 • **UNKNOWN** – Security properties of the SGX Platform Service cannot be verified due to unrecognized PSE Manifest. 由于无法识别 PSE 清单，无法验证 SGX 平台服务的安全属性。

		• **INVALID** – Security properties of the SGX Platform Service are invalid. SP should assume the SGX Platform Service utilized by the ISV enclave is invalid. SGX 平台服务的安全属性无效。SP 应该假设 ISV enclave 使用的 SGX 平台服务是无效的。 • **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. SGX 平台服务的 TCB 级别已过时，但该服务尚未被确定为受危害的，因此未被撤销。由 SP 决定是否假设 ISV enclave 使用的 SGX 平台服务是有效的。 • **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. 涉 SGX 平台服务中涉及的硬件/固件组件已被撤销。SP 应该假设 ISV enclave 使用的 SGX 平台服务是无效的。 • **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. 在 SGX 平台服务初始化过程中用于验证 SGX 平台服务中涉及的硬件/固件组件的特定类型的吊销列表已过期。如果 SP 拒绝远程认证，并通过 ISV SGX 应用程序将平台信息块转发给 SGX 平台软件，则 SGX 平台软件将尝试刷新 SGX 平台服务。 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 or CONFIGURATION_NEEDED. 此字段是可选的，只有当 SGX 平台服务安全属性描述符 (pseManifest)在认证证据有效负载中提供，并且 isvEnclaveQuoteStatus 等于 OK、GROUP_OUT_OF_DATE 或 CONFIGURATION_NEEDED 时才会出现。
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. SHA-256 通过 SGX 平台服务安全属性描述符计算得出，该描述符在认证证据有效负载中接收。该字段使用 Base 16 编码方案进行编码。

		This field is ***optional***, it will only be present if pseManifest field is provided in Attestation Evidence Payload. 此字段是可选的，只有在认证证据有效负载中提供 pseManifest 字段时才会出现。
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. 包含一个不透明二进制 blob 的 TLV，服务提供者和 ISV SGX 应用程序应该将其转发给 SGX 平台软件。该字段使用 Base 16 编码方案进行编码。 This field is ***optional***, it will only be present if one the following conditions is met: 此字段是可选的，只有在满足下列条件之一时才会出现: • isvEnclaveQuoteStatus is equal to GROUP_REVOKED, GROUP_OUT_OF_DATE or CONFIGURATION_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. 表示 SP 在验证证据有效负载中提供的 nonce 值的字符串。 This field is ***optional***, it will only be present if nonce field is provided in Attestation Evidence Payload. 此字段是可选的，仅当 nonce 字段在认证有效负载中提供时才会出现。
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. 表示 EPID 假名的字节数组，由 EPID 签名的 EPID B(64 字节)和 EPID K(64 字节)组件的连接组成。如果 EPID 组的两个可链接的 EPID 签名具有相同的 EPID 假名，则使用相同的 EPID 私钥生成这两个签名。该字段使用 Base 64 编码方案进行编码。 This field is ***optional***, it will only be present if Attestation Evidence Payload contains Quote with *linkable* EPID signature. 此字段是可选的，仅当认证证据有效负载包含带有可链接 EPID 签名的引用时才会出现。

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 XIASReport-Signature.

认证验证报告由报告签名密钥(属于认证服务)使用 RSA-SHA256 算法进行加密签名。 签名是在 HTTP 响应的整个主体上计算的。 然后，在自定义 HTTP 响应头 XIASReport-Signature 中返回 Base 64 编码的签名。

In order to verify the signature over the report the following steps must be performed:

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.

为了验证报告的签名，必须执行以下步骤:

1. 解码并验证与报告一起发送的报告签名证书链(有关详细信息，请参阅报告签名证书链)。验证此证书链是根植于可信的认证报告签署 CA 证书(成功注册到 IAS 后可下载)。
2. 可选地，验证此链中的证书没有被撤销(使用证书中指示的 CRL)。
3. 使用认证报告签名证书对报告进行签名验证。

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:
报告密钥的公共部分以 x.509 数字证书的形式分发，称为认证报告签名证书。 它是由认证报告签名 CA 证书颁发的叶证书：

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.
由认证报告签名证书和认证报告签名 CA 证书组成的 PEM 编码证书链在自定义 HTTP 响应头 X-IASReport-Signing-Certificate 中返回。

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.

平台信息块(Platform Info Blob) TLV 包含一个不透明的数据结构，要从服务提供者转发到 ISV SGX 应用程序。然后 ISV SGX 应用程序可以调用 SGX SDK API: sgx_report_attestation_status()进行分析。在内部，平台信息块 TLV 是一组状态标志和平台 TCB 信息的集合，这些信息包装在一个 TLV 容器中(其中包含一个头)。所有 TLV 头组成字段均以大端表示。

4.2.4.1 Platform Info Blob TLV

Name		**Size**(Bytes)	**Description**
TLV Header	Type	1	Identifier of Platform Info Blob TLV (*value: 21*). 平台信息块 TLV 的标识符（值：21）。
	Version	1	Version of the data structure (*value: 1 or 2*). 数据结构的版本（值：1 或 2）。
	Size	2	The size of TLV Payload data that follows this field. 此字段后面的 TLV Payload 数据的大小。
TLV Payload	Platform Info Blob	variable	Platform Information Blob to be processed by SGX Platform SW. 平台信息块数据，由 SGX 平台软件处理。

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) 此结构的版本。(小端整数) • Value: 1 or 2
	SIGNATURE_TYPE	2	2	Type of the signature. 签名类型。 Bit 0: 0 – unlinkable 1 – linkable Other bits reserved. 其他位保留。
	GID	4	4	ID of platform’s EPID Group. (Little-endian integer) 平台 EPID 组的 ID。(小端整数)
	ISVSVN_QE	8	2	The security version of the QE. (Little-endian integer) QE(Quoting Enclave)的安全版本号。(小端整数)
	ISVSVN_PCE	10	2	The security version of the PCE. (Little-endian integer) PCE 的安全版本号。(小端整数) This field is filled only in case of QUOTE with VERSION set to 2. 仅当 QUOTE 的版本设置为 2 时才填充此字段。

				In case of QUOTE with VERSION set to 1, it is 0'ed. 如果 QUOTE 的版本设置为 1，则为 0。
	RESERVED	12	4	Reserved bytes (set to 0).
	BASENAME	16	32	EPID basename used in Quote. Quote 中使用的 EPID 基名。
REPORTBODY	CPUSVN	48	16	The security version of the CPU represented as a byte array. 用字节数组表示的 CPU 的安全版本号。
	MISCSELECT	64	4	SSA frame extended feature set for the enclave. (Little-endian integer) 用于 Enclave 的 SSA 帧扩展功能集。(小端整数)
	RESERVED	68	28	Reserved bytes (set to 0).
	ATTRIBUTES	96	16	The values of the attributes flags for the enclave. 安全区(Enclave)的属性标志的值。
	MRENCLAVE	112	32	Enclave measurement represented as SHA256 digest (as defined in FIPS PUB 180-4). Enclave 度量的 SHA256 摘要(在 FIPS PUB 180-4 中定义)表示形式。
	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. Enclave 签名密钥对的 RSA 公钥的大端格式模数的 SHA256 摘要(如 FIPS PUB 180-4 中定义)。
	RESERVED	208	96	Reserved bytes (set to 0).
	ISVPRODID	304	2	Enclave Product ID. (Little-endian integer) Enclave 产品 ID。(小端整数)
	ISVSVN	306	2	The security version of the enclave. (Little-endian integer) Enclave 的安全版本号。(小端整数)
	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(). GetQuote()的 REPORT 输入中的 REPORT.ReportData 的值或 GetQuote()的 NB_UD 输入中的 UserData 的值。
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) 以字节为单位的 SIG 字段长度。SIG_LEN 不是被签名数据的一部分。(小端整数)
SIG		436	variable	Encrypted EPID signature over BODY and REPORTBODY. 对 BODY 和 REPORTBODY 的加密 EPID 签名。

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.

SGX 平台服务安全属性描述符是平台提供的一个不透明的 256 字节数据结构。