Intel® SGX and Intel® TDX Provisioning Certification Service Migration Guide API v3 -> v4

Since 2021 the Intel® SGX and Intel® TDX Provisioning Certification Service (Intel PCS) provides API endpoints in version 4 (v4). In this guide, we present important changes compared to the API endpoints in version 3 (v3), which should be used to migrate from v3 to v4.

In Section 1, we describe the changes to Intel PCS. In Section 21, we describe what PCCS users should consider. In Section 3, we describe what PCKIDRetrievalTool, QPL, and QvE/QVL users should consider.

Note that the v3 API endpoints are deprecated and will be removed at a certain point. Details about the removal are communicated separately.

1 Provisioning Certification Service

1.1 Changes to Multiple Endpoints

1.1.1 Introduction of Advisory IDs List

Since v2 of the Intel PCS API, the following API endpoints optionally contain a field called *advisoryIDs*:

- Retrieve TCB Info
- Retrieve QE Identity
- Retrieve QVE Identity
- Retrieve QAE Identity

In v2 and v3, the field is not filled.

In v4, this field can now contain a list of strings of two types: Advisory IDs and/or Intel Doc IDs. Both types are described in the following.

Advisory IDs

A collection of strings representing Advisory IDs (e.g., INTEL-SA-00075, INTEL-SA-00076) relevant to a given TCB level, describing potential vulnerabilities that this TCB level is vulnerable to.

Advisories can be searched on Intel® Product Security Center Advisories page:
https://www.intel.com/content/www/us/en/security-center/default.html

Intel Doc IDs

A collection of strings representing Intel Doc IDs (e.g. INTEL-DOC-10000, INTEL-DOC-10001) relevant to a given TCB level. The corresponding documents contain additional information about the attested platform.

The articles referred by Doc IDs can be found under the following URL:
https://api.portal.trustedservices.intel.com/documents/{INTEL-DOC-XXXXX}

1.2 Changes to Individual Endpoints

The following table explains the main differences between v3 and v4 of the API. For more details of the individual endpoints, see the online API description at https://api.portal.trustedservices.intel.com/content/documentation.html.

Category	Endpoint	Version 3	Version 4	Details
API	Retrieve PCK Certificate HTTP GET	-	**New HTTP response headers in 400 Bad Request:** Error-Code Error-Message	The additional headers are added for troubleshooting purposes – they may help to investigate potential issues in an invalid request. See the definition of response headers in Appendix A for details about the format.
		-	**New HTTP response status code 429 Too Many Requests and corresponding HTTP header:** Retry-After	New HTTP status code and header returned when the client has exceeded the limit of requests in a given amount of time. Header will define an amount of time (in seconds) to wait before the next request can be sent.
		Mandatory HTTP request header: Ocp-Apim-Subscription-Key	**Optional HTTP request header:** Ocp-Apim-Subscription-Key	A subscription key is no longer necessary allowing anonymous access. However, all customers using anonymous access share the same rate limit (see row above for more details about rate limit). Using your own subscription key is recommended as this results in a separate rate limit.

	Retrieve PCK Certificates HTTP GET	-	**New HTTP response headers in 400 Bad Request:** Error-Code Error-Message	The additional headers are added for troubleshooting purposes – they may help to investigate potential issues in an invalid request. See the definition of response headers in Appendix A for details about the format.
		-	**New HTTP response status code 429 Too Many Requests and corresponding HTTP header:** Retry-After	New HTTP status code and header returned when the client has exceeded the limit of requests in a given amount of time. Header will define an amount of time (in seconds) to wait before the next request can be sent.
		Mandatory HTTP request header: Ocp-Apim-Subscription-Key	**Optional HTTP request header:** Ocp-Apim-Subscription-Key	A subscription key is no longer necessary allowing anonymous access. However, all customers using anonymous access share the same rate limit (see row above for more details about rate limit). Using your own subscription key is recommended as this results in a separate rate limit.
	Retrieve TCB Info HTTP GET	**HTTP response header:** SGX-TCB-Info-Issuer-Chain	**HTTP response header:** TCB-Info-Issuer-Chain	The name of header containing the issuer certificate chain changed, because it is now additionally used for Intel TDX. The header consists of the SGX Root CA Certificate and the SGX TCB Signing

				Certificate, which is used for Intel SGX and Intel TDX.
		HTTP response body: TCB Info version 2	**HTTP response body:** TCB Info version 3	The structure of the responded TCB Info changed. See Section 1.3.11.3.1 for details. The response contains TCB information for given FMSPC for Intel SGX and Intel TDX.
		Request (Intel SGX): /sgx/certification/v3/tcb?fmspc={fmspc}	**Request (Intel SGX):** /sgx/certification/v4/tcb?fmspc={fmspc} **Request (Intel TDX):** /tdx/certification/v4/tcb?fmspc={fmspc}	The request URL changed to v4 and a dedicated endpoint for Intel TDX was added. The endpoints are used to retrieve TCB information for given FMSPC for Intel SGX or Intel TDX.
	Retrieve QE Identity HTTP GET	**Request (Intel SGX):** /sgx/certification/v3/qe/identity	**Request (Intel SGX):** /sgx/certification/v4/qe/identity **Request (Intel TDX):** /tdx/certification/v4/qe/identity	The request URL changed to v4 and a dedicated endpoint for Intel TDX was added. The endpoints are used to retrieve identity information for the Intel SGX/TDX Quoting Enclave issued by Intel.
	Retrieve FMSPCs HTTP GET	-	**Request:** /sgx/certification/v4/fmspcs?platform={platform}	The endpoint was added. The endpoint is used to retrieve a list of FMSPC values for platforms supporting Intel SGX and Intel TDX and DCAP-based attestation.
	Retrieve TCB Evaluation Data Numbers	-	**Request (Intel SGX):** /sgx/certification/v4/tcbevaluationdatanumbers	The endpoints were added. The endpoints are used to retrieve a list of currently supported TCB Evaluation

	HTTP GET		**Request (Intel TDX):** /tdx/certification/v4/tcbevaluationdatanumbers	Data Numbers and associated TCB-R event dates.

1.3 Changes to Data Structures

1.3.1 TCB Info Structure

Field name	**Version 2**	**Version 3**	**Details**
tcbInfo	-	id	Added field defining to which technology this TCB Info belongs to. Supported values: 1. *SGX* 2. *TDX*
	-	tdxModule	Properties of the Intel TDX Module for TDX 1.0 (TDX Module major version 0). See Section 1.4.2 for details. This field is only present in TCB Info for Intel TDX.
	-	tdxModuleIdentities	List of information about Intel TDX Modules for TDX 1.5 and above (TDX Module major version 1 and above). See Section 1.4.3 for details. This field is only present in TCB Info for Intel TDX.
	tcbLevels	tcbLevels	Sorted list of supported TCB levels for a given FMSPC. The structure of the TCB Levels changed (see Section 1.3.2).

1.3.2 TCB Level List

Version 2			Version 3		
Field name		**Details**	**Field name**		**Details**
tcb	**sgxtcbcomp01svn**	SGX TCB Component 01 SVN.	**tcb**	**sgxtcbcomponents**	Array of 16 TCB Components related to Intel SGX (as in CPUSVN). Encoded as a JSON array of TCB Component objects.
	sgxtcbcomp02svn	SGX TCB Component 02 SVN.		**tdxtcbcomponents**	Array of 16 TCB Components related to Intel TDX (as in TEE TCB SVN array in TD Report). Encoded as a JSON array of TCB Component objects. This field is only present in TCB Info for Intel TDX.
	…	…			
	sgxtcbcomp16svn	SGX TCB Component 16 SVN.			
	pcesvn	PCE SVN.		**pcesvn**	PCE SVN.
N/A			**advisoryIDs**		Array of Advisory IDs describing vulnerabilities that this TCB Level is vulnerable to and/or Doc IDs with additional information about the attested platform. This field is ***optional***. It will be present only if the list is not empty.

1.4 New Data Structures

1.4.1 TCB Component

Field name	Details
svn	SVN of TCB Component.
category	Category of TCB Component. This field is ***optional*** and will be present only for selected TCB Components**.**
type	Type of TCB Component. This field is ***optional*** and will be present only for selected TCB Components**.**

1.4.2 Intel TDX Module

Field name	Details
mrsigner	Base 16-encoded string representation of the measurement of the signing key used for the Intel TDX Module. Note that this is only used for 3rd Paty Intel TDX Modules and 0 for all Intel provided Intel TDX Modules.
attributes	Hex-encoded byte array (8 bytes) representing the attributes of the Intel TDX Module. Note that this is only used for 3rd Paty Intel TDX Modules and 0 for all Intel provided Intel TDX Modules.
attributesMask	Hex-encoded byte array (8 bytes) representing mask to be applied to the attributed of the Intel TDX Module retrieved from the platform.

1.4.3 Intel TDX Module Identity

Field name	Details
id	Identifier of the Intel TDX Module issued by Intel.
mrsigner	Base 16-encoded string representation of the measurement of the signing key used for the Intel TDX Module. Note that this is only used for 3rd Paty Intel TDX Modules and 0 for all Intel provided Intel TDX Modules.
attributes	Hex-encoded byte array (8 bytes) representing the attributes of the Intel TDX Module. Note that this is only used for 3rd Party Intel TDX Modules and 0 for all Intel provided Intel TDX Modules.
attributesMask	Hex-encoded byte array (8 bytes) representing mask to be applied to the attributed of the Intel TDX Module retrieved from the platform.
tcbLevels	Sorted list of supported TCB Levels for given Intel TDX Module encoded as a JSON array of TDX Module TCB level objects (see Section 1.4.4).

1.4.4 Intel TDX Module TCB level

Field name		Details
tcb	isvsvn	Intel TDX Module's ISV SVN.
tcbDate		Representation of date and time when the TCB Level was certified not to be vulnerable to any issues described in SAs that were published on or prior to this date. The time shall be in UTC and the encoding shall be compliant to ISO 8601 standard (YYYY-MM-DDThh:mm:ssZ).
tcbStatus		TCB Level status. One of the following values: • UpToDate • OutOfDate • Revoked
advisoryIDs		Array of strings in the following formats: - "INTEL-SA-XXXXX" (where XXXXX is a placeholder for a 5-digit number) - representing Security Advisories that can be searched on Intel® Product Security Center Advisories page (https://www.intel.com/content/www/us/en/security-center/default.html) - "INTEL-DOC-XXXXX" (where XXXXX is a placeholder for a 5-digit number) - representing articles containing additional information about the attested TDX Module. The articles can be found under the following URL: https://api.portal.trustedservices.intel.com/documents/{INTEL-DOC-XXXXX} These strings references documents that contain information specific to the given Intel TDX Module. They provide insight into the reasons for TCB Level status when the value is not UpToDate. This field is optional. It will only be present if a Security Advisory or Document for this Intel TDX Module version exists.

2 Provisioning Certification Caching Service (PCCS)

This section only applies to customers using the PCCS for collateral caching.

Migration steps:

- [**Recommended**] Backup old database.
- Install new version of PCCS (1.14 or newer), which will automatically perform the migration.
- Update the PCCS configuration file to use v4 in the uri field:
    - "uri": "https://api.trustedservices.intel.com/sgx/certification/v4/",

3 PCKIDRetrievalTool, QPL, and QvE/QVL

This section only applies to customers using listed tools from the DCAP software stack.

3.1 PCKIDRetrievalTool

Migration steps:

- Use at least version 1.14.
- In the tool's configuration file (network_setting.conf), use v4 in the PCCS URL. For example:
    - PCCS_URL=https://localhost:8081/sgx/certification/v4/platforms
- Alternatively, use the command line parameter "--url" and to reach out to the v4 endpoint of your collateral caching service (e.g., PCCS).

3.2 QPL

Migration steps:

- Use at least version 1.14 of the DCAP software stack.
- Set the v4 endpoint as PCCS URL, e.g., PCCS_URL=https://localhost:8081/sgx/certification/v4/platforms in the tool's configuration.
    - Linux: Configuration done in file /etc/sgx_default_qcnl.conf.
      Windows: Configuration done via registry key [HKEY_LOCAL_MACHINE\SOFTWARE\Intel\SGX\QCNL].

3.3 QvE/QVL

Migration steps:

- Use at least version 1.14 of the DCAP software stack.

Appendix A: 400 Bad Request – Additional Headers

Error	Message
InvalidRequestSyntax	The request could not be understood by the server due to malformed syntax.
InvalidRegistrationServer	The request was rejected by the server as it is intended to be processed by a different instance of Registration Server (Registration Server Authentication Key mismatch).
InvalidOrRevokedPackage	The request was rejected by the server due to an invalid or revoked processor package.
PackageNotFound	The request was rejected by the server as at least one of the processor packages could not be recognized by the server.
IncompatiblePackage	The request was rejected by the server as at least one of the processor packages is incompatible with rest of the processor packages forming the platform.
InvalidPlatformManifest	The request was rejected by the server due to invalid platform configuration.

Appendix B: Optional Update and TCB Evaluation Data Number parameters

The TCB Info and Enclave Identity endpoints now allow you to request a specific version of the collateral using the “update” and “tcbEvaluationDataNumber” parameters. Both parameters are optional, cannot be provided at the same time, and are present in v3 and v4 of the API.

For more details check this post and this article.