Provisioning Certification Service for Intel® SGX and Intel® TDX: API V3 -> V4 migration guide

1. Provisioning Certification Service

This document introduces changes that you should be aware of when switching from PCS API version 3 to version 4.

1.1 Summary of changes in API v4

Added Intel® Trust Domain Extensions (Intel® TDX) Support

For a detailed description of the Intel TDX API, please visit the Intel® Software Guard Extensions (Intel® SGX) API Portal: https://api.portal.trustedservices.intel.com/documentation

Introduced Vulnerable Advisory IDs

Advisory IDs refer to Intel security advisories that provide insight into the reason(s) for the value of "tcbStatus" for a specific TCB level, when the value is not "UpToDate".

Advisory IDs may occur in the following APIs:

- *Retrieve SGX/TDX TCB Info*
- *Retrieve QE Identity*
- *Retrieve QVE Identity*

Added Optional Subscription

API v4 can have anonymous (no client authentication required) access to the following APIs:

- *Retrieve PCK Certificate,*
- *Retrieve PCK Certificates,*
- *Retrieve PCK Certificates for config.*

API key header (Ocp-Apim-Subscription-Key) is now optional:

- If it is not provided, anonymous access is assumed
- If it is provided, client gets authenticated (same as v3)

It is still recommended to use your API key if you have one to have separate rate limit instead of shared one among other anonymous users (see API Throttling).

Added API Throttling

A limit to the number of API requests has been introduced. Changes described in table below are related to the following APIs:

- *Retrieve PCK Certificate*
  - HTTP GET/POST /sgx/certification/v4/pckcert
- *Retrieve PCK Certificates*
  - HTTP GET/POST /sgx/certification/v4/pckcerts
- *Retrieve PCK Certificates for config*
  - HTTP POST /sgx/certification/v4/pckcerts/config

Status Code	Version 3	Version 4
429 Too Many Requests	N/A	The client has exceeded the limit of requests in a given amount of time. Response header **Retry-After** will contain a number of seconds in which we should retry request.

1.2 Table below introduces changes to be aware of when switching from V3 to V4.

For a more detailed API description, visit the SGX API Portal:
https://api.portal.trustedservices.intel.com/documentation

Difference	Version 3	Version 4	Details
Retrieve TCB Info HTTP GET	**Response header:** SGX-TCB-Info-Issuer-Chain	**Response header:** TCB-Info-Issuer-Chain	Issuer Certificate chain for SGX/TDX TCB Info. It consists of SGX Root CA Certificate and SGX TCB Signing Certificate.
Retrieve TCB Info HTTP GET	**Response:** TCB Info version 2	**Response:** TCB Info version 3	Retrieve SGX or TDX TCB information for given FMSPC.
Retrieve TCB Info HTTP GET	**Request (SGX):** /sgx/certification/v3/tcb?fmspc={fmspc}	**Request (SGX):** /sgx/certification/v4/tcb?fmspc={fmspc}	Retrieve SGX or TDX TCB information for given FMSPC.

		Request (TDX): /tdx/certification/v4/tcb?fmspc={fmspc}	
Retrieve QE Identity HTTP GET	**Request (SGX):** /sgx/certification/v3/qe/identity	**Request (SGX):** /sgx/certification/v4/qe/identity **Request (TDX):** /tdx/certification/v4/qe/identity	Retrieve Quote Identity information for Quoting Enclave issued by Intel.
Retrieve QE Identity HTTP GET	N/A	**Response:** New field: advisoryIDs	Array of Advisory IDs describing vulnerabilities that this TCB level of an enclave is vulnerable to. This list contains SAs specific to given SGX Enclave. This field is optional.
Retrieve FMSPCs HTTP GET	-	**Request:** /sgx/certification/v4/fmspcs?platform={platform}	Retrieve list of FMSPC values for SGX and TDX platforms supporting DCAP attestation. Optional query parameter {platform} supports following values: • ALL • CLIENT • E3 • E5 When not provided, ALL is assumed.

1.3 Additional headers for HTTP 400 Bad Request

Changes described in tables below are related to the following APIs:

- *Retrieve PCK Certificate*
  HTTP GET/POST /sgx/certification/v4/pckcert
- *Retrieve PCK Certificates*
  HTTP GET/POST /sgx/certification/v4/pckcerts
- *Retrieve PCK Certificates for config*
  HTTP POST /sgx/certification/v4/pckcerts/config

Status Code	Version 3	Version 4	Details
400 Bad Request	N/A	Additional details about the error condition that occurred are returned to the client in the response headers: **Error-Code** and **Error-Message** (see the definition of response headers for details about the format).	The additional headers are added for troubleshooting purposes - they may help to investigate potential issues in an invalid request.

Response Headers:

Error-Code	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 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.

1.4 TCB Info structure

Field name	Version 2	Version 3	Details
tcbInfo	-	id	Identifier of the TCB Info issued by Intel. Supported values: 1. SGX 2. TDX
	version	version	Version of the structure.
	issueDate	issueDate	Representation of date and time the TCB information was created.
	nextUpdate	nextUpdate	Representation of date and time by which next TCB information will be issued.
	fmspc	fmspc	Base 16-encoded string representation of FMSPC (Family-Model-Stepping-Platform-CustomSKU).
	pceId	pceId	Base 16-encoded string representation of PCE Identifier.
	tcbType	tcbType	Type of TCB level composition that determines TCB level comparison logic.
	tcbEvaluationDataNumber	tcbEvaluationDataNumber	A monotonically increasing sequence number changed when Intel updates the content of the TCB evaluation data set: TCB Info, QE Identity and QVE Identity.
	-	tdxModule	Representation of the properties of Intel's TDX SEAM module. This field is *optional* and only present in TDX TCB Info.
	tcbLevels	tcbLevels	Sorted list of supported TCB levels for given FMSPC. Differences between TCB Info v2 and v3.
signature			Base 16-encoded string representation of signature.

1.4.1 TCB Levels structure

Version 2			**Version 3**		
Field name		**Details**	**Field name**		**Details**
tcb	**sgxtcbcomp01svn**	SGX TCB Component 01 SVN.	**tcb**	**sgxtcbcomponents**	Array of 16 SGX TCB Components (as in CPUSVN) encoded as a JSON array of TCB Component objects.
	sgxtcbcomp02svn	SGX TCB Component 02 SVN.		**tdxtcbcomponents**	Array of 16 TDX TCB Components (as in TEE TCB SVN array in TD Report) encoded as a JSON array of TCB Component objects. This field is ***optional*** and only present in TDX TCB Info.
	…	…			
	sgxtcbcomp16svn	SGX TCB Component 16 SVN.			
	pcesvn	PCE SVN.		**pcesvn**	PCE 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.	**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.
tcbStatus		TCB level status.	**tcbStatus**		TCB level status.
N/A			**advisoryIDs**		Array of Advisory IDs describing

					vulnerabilities that this TCB level is vulnerable to. This field is ***optional***. It will be present only if the list of Advisory IDs is not empty.

1.4.2 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 select TCB Components**.**
type	Type of TCB Component. This field is ***optional*** and will be present only for select TCB Components**.**

1.4.3 TDX Module

Field name	Details
mrsigner	Base 16-encoded string representation of the measurement of a TDX SEAM module's signer.
attributes	Hex-encoded byte array (8 bytes) representing attributes "golden" value.
attributesMask	Hex-encoded byte array (8 bytes) representing mask to be applied to TDX SEAM module's attributes value retrieved from the platform.

2. Provisioning Certification Caching Service

(applies only to customers who use PCCS - PCCS README on GitHub)

Recommendation: Back up old database before updating.

Install new version (1.14 or newer).

Migration is automatic, there are no other required steps.

Please make sure for the configuration file (**default.json**), you need to use v4 version URI:

"uri": "https://api.trustedservices.intel.com/sgx/certification/v4/",

3. PCKIDRetrievalTool and QPL

(Applies only to customers who use DCAP software stack - DCAP README on GitHub)

3.1. PCKIDRetrievalTool

Please use version 1.14 or newer.

In this tool's configuration file (**network_setting.conf**), you need to use V4 version **PCCS_URL**:

 # support V4 version PCCS

PCCS_URL=https://localhost:8081/sgx/certification/v4/platforms

Or if you use command line parameter: **--url**, please make sure you are using v4 version cache server.

3.2. QPL

Please use DCAP software stack from version 1.14 or newer.

3.2.1 Linux

For Linux, make sure you provide V4 version of **pccs_url** in the configuration file in default location **/etc/sgx_default_qcnl.conf**:

// PCCS server address

"pccs_url": "https://localhost:8081/sgx/certification/v4/",

3.2.2 Windows

In Windows, you can check or specify the location of the configuration file through the registry key:

[HKEY_LOCAL_MACHINE\SOFTWARE\Intel\SGX\QCNL]

You need to provide V4 version of **pccs_url** in your configuration file.

// PCCS server address

"pccs_url": "https://localhost:8081/sgx/certification/v4/",