

Intel® Software Guard Extensions: PCK Certificate and Certificate Revocation List Profile Specification

**Rev 1.1
January 8, 2019**



Copyright © Intel Corporation 2007 – 2019

Table of Contents

1. Introduction.....	3
1.1. Terminology.....	3
1.2. References	3
2. Certificate Hierarchy.....	4
2.1. Certificates.....	4
2.2. Certificate Revocation Lists.....	5
3. Certificate Formats.....	6
3.1. Intel® Software Guard Extensions Root CA Certificate.....	6
3.2. Intel® SGX PCK Platform CA Certificate.....	6
3.3. Intel® SGX PCK Processor CA Certificate	7
3.4. Intel® SGX TCB Signing Certificate	8
3.5. Intel® SGX PCK Certificate.....	8
4. Certificate Revocation List Formats	11
4.1. Intel® SGX Root CA CRL	11
4.2. Intel® SGX PCK Platform CA CRL.....	11
4.3. Intel® SGX PCK Processor CA CRL	11
5. Appendices	13
5.1. Appendix A: Profile for Specific Certificate Extensions for the Intel® Software Guard Extensions.....	13

1.Introduction

This document specifies the hierarchy and format of X.509 v3 certificates and X.509 v2 Certificate Revocation Lists (CRLs) issued by Intel for Provisioning Certification Keys. Certificates and CRLs use a standard set of extensions described in the document. Additionally, a number of PCK-specific extensions are defined.

1.1.Terminology

Provisioning Certification Enclave (PCE)	Intel® Software Guard Extensions (Intel® SGX) enclave that uses a Provisioning Certification Key to sign proofs that attestation keys or attestation key provisioning protocol messages are created on genuine hardware.
Provisioning Certification Key (PCK)	Signing key available to a Provisioning Certification Enclave (PCE). The key is unique to the processor package or platform instance and its Trusted Computing Base (HW and PCE). The public part of the key is distributed as a PCK Certificate.
Platform Provisioning ID (PPID)	Unique Provisioning ID of the processor package or platform instance. The PPID does not depend on the Trusted Computer Base (TCB).
Trusted Computing Base (TCB)	Set of hardware and software components that are critical to the security of the solution.
Security Version Number (SVN)	Version number of a component that indicates when security relevant updates have been applied to the component. The SVN might not correlate with the functional version of the component.
Family-Model-Stepping-Platform-CustomSKU (FMSPC)	Description of the processor package or platform instance including its Family, Model, Stepping, Platform Type, and Customized SKU (if applies).

Table 1-1: Terminology

1.2. References

RFC 4648 (Base16, Base32 and Base64)	October 2006	http://www.ietf.org/rfc/rfc4648.txt
RFC 5280 (X.509 Certificate and CRL)	May 2008	http://tools.ietf.org/html/rfc5280

Table 1-2: References

2. Certificate Hierarchy

The figure below illustrates the hierarchy of PCK certificates and CRLs issued by Intel. High level description of all the certificates and CRLs that are part of the hierarchy can be found in the 2.1 Certificates and 2.2 Certificate Revocation Lists tables.

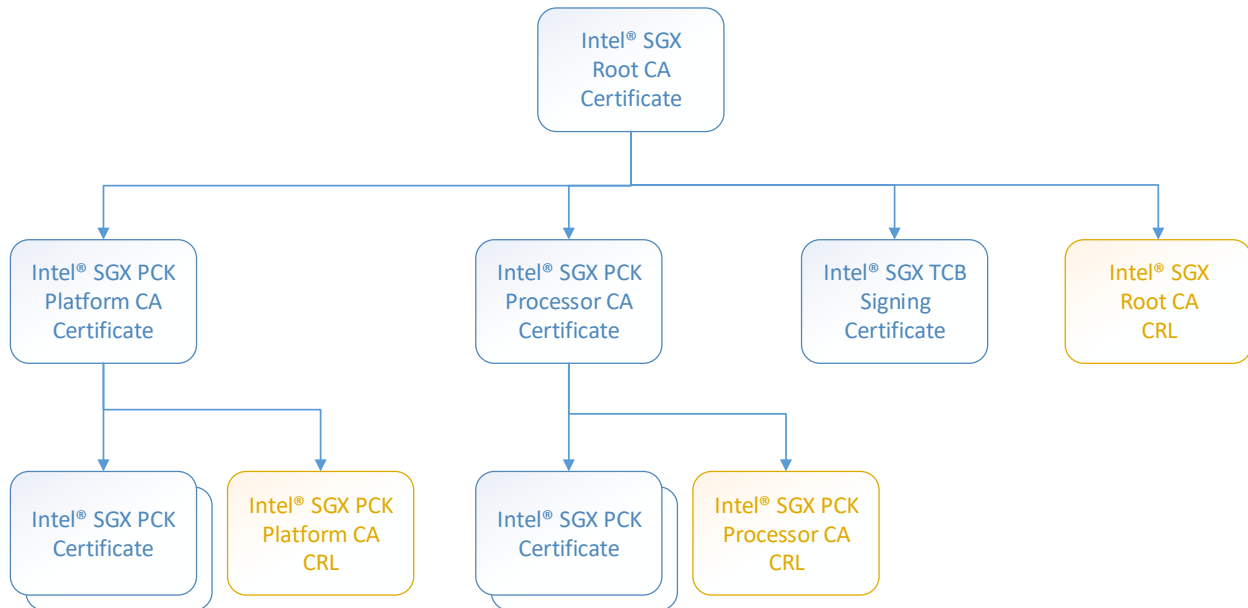


Figure 2-1: Certificate Hierarchy

2.1. Certificates

Certificate	Description
Intel® SGX Root CA Certificate	Intel® self-signed root Certificate Authority (CA) certificate (in X.509 format as defined in RFC 5280) that is designated to issue certificates related to Intel® Software Guard Extensions (Intel® SGX). <i>For more details see: Intel® SGX Root CA Certificate.</i>
Intel® SGX PCK Platform CA Certificate	Intermediate CA certificate (in X.509 format as defined in RFC 5280) that issues Intel® SGX PCK Certificates and corresponding CRLs for multi-package platforms. Currently not supported. <i>For more details see: Intel® SGX PCK Platform CA Certificate.</i>
Intel® SGX PCK Processor CA Certificate	Intermediate CA certificate (in X.509 format as defined in RFC 5280) that issues Intel® SGX PCK Certificates and corresponding CRLs for single-package platforms.

	<p>For more details see: Intel® SGX PCK Processor CA Certificate.</p>
Intel® SGX TCB Signing Certificate	<p>Leaf certificate (in X.509 format as defined in RFC 5280) that signs the Intel® SGX TCB data for Intel® platforms (both single and multi-package).</p> <p>For more details see: Intel® SGX TCB Signing Certificate.</p>
Intel® SGX PCK Certificate	<p>Leaf certificate (in X.509 format as defined in RFC 5280) that contains a public part of a PCK for an Intel® SGX platform on a specific TCB level.</p> <p>For more details see: Intel® SGX PCK Certificate.</p>

Table 2-1: Certificates

2.2. Certificate Revocation Lists

Certificate Revocation List	Description
Intel® SGX Root CA CRL	<p>Certificate Revocation List (in X.509 format as defined in RFC 5280) issued by the Intel® SGX Root Certification Authority (CA).</p> <p>For more details see: Intel® SGX Root CA CRL.</p>
Intel® SGX PCK Platform CA CRL	<p>Certificate Revocation List (in X.509 format as defined in RFC 5280) issued by the Intel® SGX PCK Platform CA.</p> <p>Currently not supported.</p> <p>For more details see: Intel® SGX PCK Platform CA CRL.</p>
Intel® SGX PCK Processor CA CRL	<p>Certificate Revocation List (in X.509 format as defined in RFC 5280) issued by the Intel® SGX PCK Processor CA.</p> <p>For more details see: Intel® SGX PCK Processor CA CRL.</p>

Table 2-2: Certificate Revocation Lists

3. Certificate Formats

All certificates described in this section follow X.509 standard (as defined in [RFC 5280](#)). Placeholders for variable values in the certificates, such as signatures, are marked as **<placeholder>**.

3.1. Intel® Software Guard Extensions Root CA Certificate

Certificate:

```
Data:
  Version: 3 (0x2)
  Serial Number:
    <serial number>
Signature Algorithm: ecdsa-with-SHA256
Issuer: CN=Intel SGX Root CA, O=Intel Corporation, L=Santa Clara, ST=CA, C=US
Validity
  Not Before: <time of issuing>
  Not After: Dec 31 2049 23:59:59 UTC
Subject: CN=Intel SGX Root CA, O=Intel Corporation, L=Santa Clara, ST=CA, C=US
Subject Public Key Info:
  Public Key Algorithm: id-ecPublicKey
  Public-Key: (256 bit)
  pub:
    <public key>
  ASN1 OID: prime256v1
X509v3 extensions:
  X509v3 Authority Key Identifier:
    keyid:<keyid of issuer public key>

  X509v3 CRL Distribution Points:

    Full Name:
      URI: <URL>

  X509v3 Subject Key Identifier:
    keyid:<keyid of public key>
  X509v3 Key Usage: critical
    Certificate Sign, CRL Sign
  X509v3 Basic Constraints: critical
    CA:TRUE, pathlen:1

Signature Algorithm: ecdsa-with-SHA256
  <signature>
```

3.2. Intel® SGX PCK Platform CA Certificate

Note: This is only a draft format, which may be changed in future Intel® Software Guard Extensions (Intel® SGX) updates.

Certificate:

```
Data:
  Version: 3 (0x2)
  Serial Number:
    <serial number>
Signature Algorithm: ecdsa-with-SHA256
Issuer: CN=Intel SGX Root CA, O=Intel Corporation, L=Santa Clara, ST=CA, C=US
Validity
```

Not Before: **<start of validity period>**
Not After : **<expiration date, should be valid for about 15 years>**
Subject: CN=Intel SGX PCK Platform CA, O=Intel Corporation, L=Santa Clara, ST=CA,
C=US

Subject Public Key Info:
Public Key Algorithm: id-ecPublicKey
Public-Key: (256 bit)
pub:
<public key>
ASN1 OID: prime256v1

X509v3 extensions:
X509v3 Authority Key Identifier:
keyid:**<keyid of issuer public key>**

X509v3 CRL Distribution Points:

Full Name:
URI: **<URL>**

X509v3 Subject Key Identifier:
<keyid of public key>
X509v3 Key Usage: critical
Certificate Sign, CRL Sign
X509v3 Basic Constraints: critical
CA:TRUE, pathlen:0

Signature Algorithm: ecdsa-with-SHA256
<signature>

3.3.Intel® SGX PCK Processor CA Certificate

Certificate:
Data:
Version: 3 (0x2)
Serial Number:
<serial number>

Signature Algorithm: ecdsa-with-SHA256
Issuer: CN=Intel SGX Root CA, O=Intel Corporation, L=Santa Clara, ST=CA, C=US
Validity
Not Before: **<start of validity period>**
Not After : **<expiration date, should be valid for about 15 years>**
Subject: CN=Intel SGX PCK Processor CA, O=Intel Corporation, L=Santa Clara,
ST=CA, C=US

Subject Public Key Info:
Public Key Algorithm: id-ecPublicKey
Public-Key: (256 bit)
pub:
<public key>
ASN1 OID: prime256v1

X509v3 extensions:
X509v3 Authority Key Identifier:
keyid:**<keyid of issuer public key>**

X509v3 CRL Distribution Points:

Full Name:
URI: **<URL>**

X509v3 Subject Key Identifier:
<keyid of public key>

X509v3 Key Usage: critical
Certificate Sign, CRL Sign
X509v3 Basic Constraints: critical
CA:TRUE, pathlen:0

Signature Algorithm: ecdsa-with-SHA256
<signature>

3.4.Intel® SGX TCB Signing Certificate

Certificate:

Data:

Version: 3 (0x2)

Serial Number:

<serial number>

Signature Algorithm: ecdsa-with-SHA256

Issuer: CN=Intel SGX Root CA, O=Intel Corporation, L=Santa Clara, ST=CA, C=US

Validity

Not Before: **<start of validity period>**

Not After : **<expiration date, should be valid for about 7 years>**

Subject: CN=Intel SGX TCB Signing, O=Intel Corporation, L=Santa Clara, ST=CA,

C=US

Subject Public Key Info:

Public Key Algorithm: id-ecPublicKey

Public-Key: (256 bit)

pub:

<public key>

ASN1 OID: prime256v1

X509v3 extensions:

X509v3 Authority Key Identifier:

keyid:**<keyid of issuer public key>**

X509v3 CRL Distribution Points:

Full Name:

URI: **<URL>**

X509v3 Subject Key Identifier:

<keyid of public key>

X509v3 Key Usage: critical

Digital Signature, Non Repudiation

X509v3 Basic Constraints: critical

CA:FALSE

Signature Algorithm: ecdsa-with-SHA256
<signature>

3.5.Intel® SGX PCK Certificate

Certificate:

Data:

Version: 3 (0x2)

Serial Number:

<serial number>

Signature Algorithm: ecdsa-with-SHA256

Issuer: CN=**<Intel SGX PCK Platform CA | Intel SGX PCK Processor CA>**, O=Intel Corporation, L=Santa Clara, ST=CA, C=US

Validity

```

Not Before: <start of validity period>
Not After : <expiration date, should be valid for about 7 years>
Subject: CN=Intel SGX PCK Certificate, O=Intel Corporation, L=Santa Clara,
ST=CA, C=US
Subject Public Key Info:
  Public Key Algorithm: id-ecPublicKey
  Public-Key: (256 bit)
  pub:
    <public key>
  ASN1 OID: prime256v1
X509v3 extensions:
  X509v3 Authority Key Identifier:
    keyid:<keyid of issuer public key>

  X509v3 CRL Distribution Points:

    Full Name:
      URI: <URL>

  X509v3 Subject Key Identifier:
    <keyid of public key>
  X509v3 Key Usage: critical
    Digital Signature, Non Repudiation
  X509v3 Basic Constraints: critical
    CA:FALSE
  <SGX Extensions OID>:
    <PPID OID>: <PPID value>
    <TCB OID>:
      <SGX TCB Comp01 SVN OID>: <SGX TCB Comp01 SVN value>
      <SGX TCB Comp02 SVN OID>: <SGX TCB Comp02 SVN value>
      ...
      <SGX TCB Comp16 SVN OID>: <SGX TCB Comp16 SVN value>
    <PCESVN OID>: <PCESVN value>
    <CPUSVN OID>: <CPUSVN value>
    <PCE-ID OID>: <PCE-ID value>
    <FMSPC OID>: <FMSPC value>
    <SGX Type OID>: <SGX Type value>

Signature Algorithm: ecdsa-with-SHA256
  <signature>

```

The table below describes custom x.509 extensions for PCK Certificates. For details about ASN.1 encoding of the extensions, refer to [Appendix A: Profile for Specific Certificate Extensions for the Intel® SGX](#).

Name	Object Identifier (OID)	Type	Description
SGX Extensions	1.2.840.113741.1.13.1	ASN.1 Sequence	Sequence of extensions specific to the Intel® Software Guard Extensions (Intel® SGX).
PPID	1.2.840.113741.1.13.1.1	ASN.1 Octet String	Value of Platform Provisioning ID. (16 bytes)

TCB	1.2.840.113741.1.13.1.2	ASN.1 Sequence	Sequence of TCB components.
SGX TCB Comp01 SVN	1.2.840.113741.1.13.1.2.1	ASN.1 Integer	Value of the Intel® SGX TCB Comp01 SVN.
SGX TCB Comp02 SVN	1.2.840.113741.1.13.1.2.2	ASN.1 Integer	Value of the Intel® SGX TCB Comp02 SVN.
...			
SGX TCB Comp16 SVN	1.2.840.113741.1.13.1.2.16	ASN.1 Integer	Value of the Intel® SGX TCB Comp16 SVN.
PCESVN	1.2.840.113741.1.13.1.2.17	ASN.1 Integer	Value of PCESVN.
CPUSVN	1.2.840.113741.1.13.1.2.18	ASN.1 Octet String	Value of CPUSVN. (16 bytes)
PCE-ID	1.2.840.113741.1.13.1.3	ASN.1 Octet String	Value of PCE-ID. (2 bytes)
FMSPC	1.2.840.113741.1.13.1.4	ASN.1 Octet String	Value of FMSPC. (6 bytes)
SGXType	1.2.840.113741.1.13.1.5	ASN.1 Enumerated	Enum representing the Intel® SGX Type. One of the following values: - Standard (0)

Table 3-1: Custom OIDs for PCK certificate.

4. Certificate Revocation List Formats

All certificate revocation lists described in this section follow X.509 standard (as defined in [RFC 5280](#)).

4.1. Intel® SGX Root CA CRL

```
Certificate Revocation List (CRL):
  Version 2 (0x1)
  Signature Algorithm: ecdsa-with-SHA256
  Issuer: CN=Intel SGX Root CA, O=Intel Corporation, L=Santa Clara, ST=CA, C=US
  Last Update: <issuing date>
  Next Update: <date of next update>
  CRL extensions:
    X509v3 CRL Number:
      <crl number>
    X509v3 Authority Key Identifier:
      keyid: <keyid of issuer public key>

  <list of revoked certificates>

  Signature Algorithm: ecdsa-with-SHA256
    <signature>
```

4.2. Intel® SGX PCK Platform CA CRL

Note: This is only a draft format, which may be changed in future Intel® Software Guard Extensions (Intel® SGX) updates.

```
Certificate Revocation List (CRL):
  Version 2 (0x1)
  Signature Algorithm: ecdsa-with-SHA256
  Issuer: CN=Intel SGX PCK Platform CA, O=Intel Corporation, L=Santa Clara, ST=CA,
C=US
  Last Update: <issuing date>
  Next Update: <date of next update>
  CRL extensions:
    X509v3 CRL Number:
      <crl number>
    X509v3 Authority Key Identifier:
      keyid: <keyid of issuer public key>

  <list of revoked certificates>

  Signature Algorithm: ecdsa-with-SHA256
    <signature>
```

4.3. Intel® SGX PCK Processor CA CRL

```
Certificate Revocation List (CRL):
  Version 2 (0x1)
  Signature Algorithm: ecdsa-with-SHA256
```

Issuer: CN=Intel SGX PCK Processor CA, O=Intel Corporation, L=Santa Clara, ST=CA,
C=US
Last Update: **<issuing date>**
Next Update: **<date of next update>**
CRL extensions:
 X509v3 CRL Number:
 <crl number>
 X509v3 Authority Key Identifier:
 keyid: **<keyid of issuer public key>**

<list of revoked certificates>

Signature Algorithm: ecdsa-with-SHA256
 <signature>

5. Appendices

5.1. Appendix A: Profile for Specific Certificate Extensions for the Intel® Software Guard Extensions

This section describes a profile for specific certificate extensions used in the Intel® SGX PCK Certificate. This section is based on the X.509 v3 certificate format and the standard certificate extensions defined in [RFC 5280](#) and uses 1988 ASN.1 syntax.

```
id-ce-sGXExtensions OBJECT IDENTIFIER ::= { 1 2 840 113741 1 13 1 }
```

```
SGXExtensions ::= SEQUENCE SIZE (1..MAX) OF SEQUENCE {  
    sGXExtensionId    SGXExtensionId,  
    sGXExtensionValue ANY DEFINED BY sGXExtensionId }
```

```
-- sGXExtensionIds for Intel SGX PCK Certificates
```

```
id-ce-sGXExtensions-pPID          OBJECT IDENTIFIER ::= { id-ce-sGXExtensions 1 }  
id-ce-sGXExtensions-tCB          OBJECT IDENTIFIER ::= { id-ce-sGXExtensions 2 }  
id-ce-sGXExtensions-pCE-ID       OBJECT IDENTIFIER ::= { id-ce-sGXExtensions 3 }  
id-ce-sGXExtensions-fMSPC        OBJECT IDENTIFIER ::= { id-ce-sGXExtensions 4 }  
id-ce-sGXExtensions-sGXType      OBJECT IDENTIFIER ::= { id-ce-sGXExtensions 5 }
```

```
SGXExtensionId ::= OBJECT IDENTIFIER ( id-ce-sGXExtensions-pPID | id-ce-sGXExtensions-  
tCB | id-ce-sGXExtensions-pCE-ID | id-ce-sGXExtensions-fMSPC | id-ce-sGXExtensions-  
sGXType)
```

```
SGXExtensionValue ::= CHOICE {  
    pPID          [0] PPID,  
    tCB           [1] TCB,  
    pCE-ID        [3] PCE-ID,  
    fMSPC         [4] FMSPC,  
    sGXType       [5] SGXType }
```

```
PPID ::= OCTET STRING (SIZE (16))
```

```
TCB ::= SEQUENCE SIZE (1..18) OF SEQUENCE {  
    tCBId    TCBId,  
    tCBValue ANY DEFINED BY tCBId }
```

```
-- tCBIds for Intel SGX PCK Certificates
```

```

id-ce-tCB-sGXTCBComp01SVN      OBJECT IDENTIFIER ::= { id-ce-sGXExtensions-tCB 1 }
id-ce-tCB-sGXTCBComp02SVN      OBJECT IDENTIFIER ::= { id-ce-sGXExtensions-tCB 2 }
id-ce-tCB-sGXTCBComp03SVN      OBJECT IDENTIFIER ::= { id-ce-sGXExtensions-tCB 3 }
id-ce-tCB-sGXTCBComp04SVN      OBJECT IDENTIFIER ::= { id-ce-sGXExtensions-tCB 4 }
id-ce-tCB-sGXTCBComp05SVN      OBJECT IDENTIFIER ::= { id-ce-sGXExtensions-tCB 5 }
id-ce-tCB-sGXTCBComp06SVN      OBJECT IDENTIFIER ::= { id-ce-sGXExtensions-tCB 6 }
id-ce-tCB-sGXTCBComp07SVN      OBJECT IDENTIFIER ::= { id-ce-sGXExtensions-tCB 7 }
id-ce-tCB-sGXTCBComp08SVN      OBJECT IDENTIFIER ::= { id-ce-sGXExtensions-tCB 8 }
id-ce-tCB-sGXTCBComp09SVN      OBJECT IDENTIFIER ::= { id-ce-sGXExtensions-tCB 9 }
id-ce-tCB-sGXTCBComp10SVN      OBJECT IDENTIFIER ::= { id-ce-sGXExtensions-tCB 10 }
id-ce-tCB-sGXTCBComp11SVN      OBJECT IDENTIFIER ::= { id-ce-sGXExtensions-tCB 11 }
id-ce-tCB-sGXTCBComp12SVN      OBJECT IDENTIFIER ::= { id-ce-sGXExtensions-tCB 12 }
id-ce-tCB-sGXTCBComp13SVN      OBJECT IDENTIFIER ::= { id-ce-sGXExtensions-tCB 13 }
id-ce-tCB-sGXTCBComp14SVN      OBJECT IDENTIFIER ::= { id-ce-sGXExtensions-tCB 14 }
id-ce-tCB-sGXTCBComp15SVN      OBJECT IDENTIFIER ::= { id-ce-sGXExtensions-tCB 15 }
id-ce-tCB-sGXTCBComp16SVN      OBJECT IDENTIFIER ::= { id-ce-sGXExtensions-tCB 16 }
id-ce-tCB-pCESVN                OBJECT IDENTIFIER ::= { id-ce-sGXExtensions-tCB 17 }
id-ce-tCB-cPUSVN                OBJECT IDENTIFIER ::= { id-ce-sGXExtensions-tCB 18 }

```

```

TCBId ::= OBJECT IDENTIFIER (id-ce-tCB-sGXTCBComp01SVN | id-ce-tCB-sGXTCBComp02SVN | id-ce-tCB-sGXTCBComp03SVN | id-ce-tCB-sGXTCBComp04SVN | id-ce-tCB-sGXTCBComp05SVN | id-ce-tCB-sGXTCBComp06SVN | id-ce-tCB-sGXTCBComp07SVN | id-ce-tCB-sGXTCBComp08SVN | id-ce-tCB-sGXTCBComp09SVN | id-ce-tCB-sGXTCBComp10SVN | id-ce-tCB-sGXTCBComp11SVN | id-ce-tCB-sGXTCBComp12SVN | id-ce-tCB-sGXTCBComp13SVN | id-ce-tCB-sGXTCBComp14SVN | id-ce-tCB-sGXTCBComp15SVN | id-ce-tCB-sGXTCBComp16SVN | id-ce-tCB-pCESVN | id-ce-tCB-cPUSVN)

```

```

TCBValue ::= CHOICE {
    sGXTCBComp01SVN    [0] INTEGER,
    sGXTCBComp02SVN    [1] INTEGER,
    sGXTCBComp03SVN    [2] INTEGER,
    sGXTCBComp04SVN    [3] INTEGER,
    sGXTCBComp05SVN    [4] INTEGER,
    sGXTCBComp06SVN    [5] INTEGER,
    sGXTCBComp07SVN    [6] INTEGER,
    sGXTCBComp08SVN    [7] INTEGER,
    sGXTCBComp09SVN    [8] INTEGER,
    sGXTCBComp10SVN    [9] INTEGER,
    sGXTCBComp11SVN    [10] INTEGER,
    sGXTCBComp12SVN    [11] INTEGER,
    sGXTCBComp13SVN    [12] INTEGER,
    sGXTCBComp14SVN    [13] INTEGER,

```

```
sGXTCBComp15SVN    [14] INTEGER,  
sGXTCBComp16SVN    [15] INTEGER,  
pCESVN              [16] INTEGER,  
cPUSVN              [17] CPUSVN }
```

```
CPUSVN ::= OCTET STRING (SIZE (16))
```

```
PCE-ID ::= OCTET STRING (SIZE (2))
```

```
FMSPC ::= OCTET STRING (SIZE (6))
```

```
SGXType ::= ENUMERATED {
```

```
    standard (0) }
```