Versioned Chip Endorsement Key (VCEK) Certificate and KDS Interface Specification

Publication # **57230** Revision: **1.00**
Issue Date: **January 2025**

Advanced Micro Devices

The information contained herein is for informational purposes only, and is subject to change without notice. While every precaution has been taken in the preparation of this document, it may contain technical inaccuracies, omissions and typographical errors, and AMD is under no obligation to update or otherwise correct this information. Advanced Micro Devices, Inc. makes no representations or warranties with respect to the accuracy or completeness of the contents of this document, and assumes no liability of any kind, including the implied warranties of noninfringement, merchantability or fitness for particular purposes, with respect to the operation or use of AMD hardware, software or other products described herein. No license, including implied or arising by estoppel, to any intellectual property rights is granted by this document. Terms and limitations applicable to the purchase or use of AMD's products are as set forth in a signed agreement between the parties or in AMD's Standard Terms and Conditions of Sale.

Trademarks

Table of Contents

Chapter 1 Introduction 6

1.1 Purpose and Scope 6

1.2 Intended Audience 6

1.3 References 6

1.4 Glossary 7

1.5 Determining the Product Name 7

Chapter 2 VCEK Certificate Trust Chain 9

2.1 Certificate Authorities 9

2.2 Downloading the CA Certificates and Certificate Revocation List (CRL) 9

2.3 ARK and ASK Certificate Definitions 10

Chapter 3 VCEK Certificate Format 12

3.1 Certificate Extensions and TCB Definitions 13

Chapter 4 VCEK Certificate Access Methods 15

4.1 Get VCEK Certificate for Specified TCB 16

4.2 Get Certificate Chain 17

4.3 Get Certificate Revocation List (CRL) 17

Chapter 5 Integration Details 18

5.1 Pre-Fetching Certificates for New TCB Values 18

List of Tables

Table 1. External References 6
Table 2. Terms and Definitions 7
Table 3. Processor Version Information Definition 8
Table 4. Values for product_name 8
Table 5. VCEK Certificate Chain 9
Table 6. Downloading CA Certificates and CRL 9
Table 7. AMD Root Key (ARK) Certificate Format 10
Table 8. AMD SEV Key (ASK) Certificate Format 11
Table 9. VCEK Certificate Fields 12
Table 10. VCEK Certificate Extensions for Family 19h (structVersion = 0) 13
Table 11. VCEK Certificate Extensions for Family 1Ah (Turin) (structVersion = 1) 14
Table 12. VCEK KDS Interface Summary 15
Table 13. Get VCEK Certificate 16
Table 14. Get Certificate Chain 17
Table 15. Get Certificate Revocation List 17

Revision History

Date	Revision	Description
January 2025	1.0	• Added API changes for products using PSN-based hardware IDs • Added support for Siena • Added support description for Turin and new TCB structure definition • Added one day of guard-band to VCEK certificate's NotValidBefore date
January 2023	0.51	• Adds row for "Genoa" product in Table 3. Values for product_name • Updates TAG for OID 1.3.6.1.4.1.3704.1.4 in Table 8. VCEK Certificate Extensions for Family 19h (structVersion = 0) • Updates table numbers throughout
October 2021	0.50	• Initial public release

Chapter 1 Introduction

1.1 Purpose and Scope

This document describes the contents of the Versioned Chip Endorsement Key (VCEK) certificate and the Key Distribution System (KDS) interface used to retrieve certificate information.

VCEK certificates are used within the context of AMD Secure Encrypted Virtualization-Secure Nested Paging (SEV-SNP) technology, the details of which are not described here. For SEV-SNP information, please refer to the specification listed in Table 1. External References.

1.2 Intended Audience

This document is intended for software developers supporting virtualized host environments that employ SEV-SNP technology and need to retrieve VCEK certificates for their secure virtual machine (VM).

1.3 References

Table 1. External References

Reference	Document
RFC 5280	Internet X.509 Public Key Infrastructure Certificate and Certificate Revocation List (CRL) Profile. *https://tools.ietf.org/html/rfc5280*
SNP ABI Publication #56860	SEV Secure Nested Paging Firmware ABI Specification: *https://www.amd.com/system/files/TechDocs/56860.pdf*
SEV API Publication #55766	Secure Encrypted Virtualization API Version 0.24: *https://www.amd.com/system/files/TechDocs/55766_SEV-KM_API_Specification.pdf*

1.4 Glossary

Table 2. Terms and Definitions

Term	Definition
ARB	**Anti-Rollback**. Methods used to prevent installation of older firmware/software that contain exploitable vulnerabilities.
ARK	**AMD Root Key**. An RSA key that acts as the root certificate authority for VCEK certificates. The ARK is unique per product, and its public key is bound to each device.
ASK	**AMD SEV Key.** The intermediate certificate authority (CA) key that issues (signs) VCEK certificates. The ASK is product specific.
ICA	**Intermediate Certificate Authority.** Part of a certificate chain between the root CA and leaf certificate (e.g., a VCEK certificate).
KDS	**Key Distribution System.** The system of hardware security modules (HSMs) and supporting hardware/software that manages various cryptographic resources including VCEK certificate generation.
PSN	**Public Serial Number.** An 8-byte random number that uniquely identifies an AMD system on a chip (SoC).
SEV	**Secure Encrypted Virtualization.** An AMD technology to encrypt the memory of a virtual machine (VM) using a unique key.
SNP	**Secure Nested Paging.** An extension of SEV features that strengthens memory encryption protections using newer hardware-based security.
SPL	**Security Patch Level**. A monotonically increasing integer used to represent a minimum-security version used in anti-rollback protection. Used interchangeably with SVN.
SVN	**Security Version Number**. A version number used to prevent rollback attacks.
TCB	**Trusted Compute Base**. A “TCB version” refers to a specific combination of versions of firmware entities that are part of the TCB (e.g., bootloader firmware, SNP firmware, CPU microcode, etc.).
VCEK	**Versioned Chip Endorsement Key**. A private Elliptic Curve Digital Signature Algorithm (ECDSA) key that is unique to each AMD chip running a specific TCB version.

1.5 Determining the Product Name

The name of the product appears in the ARK, ASK, and VCEK certificates, as well as the interface URLs. The "product_name" can be determined by executing the CPUID (EAX=1) instruction on the processor and comparing the Family/Model/Stepping (FMS) information. (See Table 3. Processor Version Information Definition and Table 4. Values for product_name.)

Table 3. Processor Version Information Definition

EAX Bits	Definition
31:28	Reserved
27:20	Extended Family ID
19:16	Extended Model ID
15:14	Reserved
13:12	Processor Type
11:8	Family ID
7:4	Model
3:0	Stepping

Table 4. Values for product_name

Family (Extended Family + Family)	**Extended Model**	**product_name**[1]
19h (0Ah + Fh)	0h	"Milan"
19h (0Ah + Fh)	1h	"Genoa"
19h (0Ah + Fh)	Ah	"Siena"[2]
1Ah (0Bh + Fh)	0h or 1h	"Turin"

[1] When used as a URL path parameter, the product_name value is case sensitive.

[2] The Siena product uses the same root keys as the Genoa design and therefore uses Genoa ARK and ASK certificates to issue VCEK certificates. If Siena is not explicitly mentioned elsewhere in this document, use Genoa details as reference.

Chapter 2 VCEK Certificate Trust Chain

This section describes data structures that are common to multiple commands.

2.1 Certificate Authorities

The VCEK certificate is rooted through a certificate chain described by the table below.

Table 5. VCEK Certificate Chain

Key	Abbr.	Algorithm	Usage
AMD Root Key	ARK	RSA 4096	Root CA. Product-specific AMD Root of Trust. Issues the ASK
AMD SEV Key	ASK	RSA 4096	Intermediate CA. Issues the VCEK certificate

For more information on the ARK and ASK, refer to Chapter 2 of the SEV API specification.

2.2 Downloading the CA Certificates and Certificate Revocation List (CRL)

Certificates for the ARK and ASK also can be found at *https://developer.amd.com/sev* or via the KDS interface described below.

All URLs are hosted at *https://kdsintf.amd.com/*.

Table 6. Downloading CA Certificates and CRL

Port	URI	Method	Description
443	/vcek/v1/{product_name*}/cert_chain	GET	Returns the product-specific CA chain. Certificates are sent in PEM format.
443	/vcek/v1/{product_name}/crl	GET	Returns list of revoked certificates as per RFC 5280. CRL is sent in DER format.

* Refer to *Section 1.5. Determining the Product Name* for product names.

2.3 ARK and ASK Certificate Definitions

Table 7. AMD Root Key (ARK) Certificate Format

Version	V3
Serial Number	0xNNNNNN

Issuer	CN = ARK-{product_name} (ex: ARK-Milan)
	O = Advanced Micro Devices
	S = CA
	L = Santa Clara
	C = US
	OU = Engineering

Signature Algorithm	RSASSA-PSS
Signature Hash Algorithm	sha384
Validity	Valid from: date of issuance Valid to: 25 years after date of issuance

Subject	CN = ARK-{product_name} (ex: ARK-Milan)
	O = Advanced Micro Devices
	S = CA
	L = Santa Clara
	C = US
	OU = Engineering

Subject Public Key Info	RSA (4096 bits)
CRL Distribution Point	URL=https://kdsintf.amd.com/vcek/v1/{product_name}/crl
Key Usage	Certificate Signing, Off-line CRL Signing, CRL Signing

Table 8. AMD SEV Key (ASK) Certificate Format

Version	V3
Serial Number	0xNNNNNN
Issuer	[Subject of ARK certificate]
Signature Algorithm	RSASSA-PSS
Signature Hash Algorithm	sha384
Validity	Valid from: date of issuance Valid to: 25 years after date of issuance

Subject	CN = SEV-{product_name} (ex: SEV-Milan)
	O = Advanced Micro Devices
	S = CA
	L = Santa Clara
	C = US
	OU = Engineering

Subject Public Key Info	RSA (4096 bits)
CRL Distribution Point	URL=https://kdsintf.amd.com/vcek/v1/{product_name}/crl
Key Usage	Certificate Signing

Chapter 3 VCEK Certificate Format

The VCEK certificate is an X.509v3 certificate as defined in RFC 5280. Each certificate is generated at the time of the request; they are not stored within the KDS.

Table 9 describes the fields of the VCEK certificate.

Table 9. VCEK Certificate Fields

Version	V3
Serial Number	Zero
Issuer	[Subject of ASK certificate]
Signature Algorithm	RSASSA-PSS
Signature Hash Algorithm	sha384
Validity	Not before: one day prior to date of issuance[*] Not after: seven years after date of issuance

Subject	CN = SEV-VCEK
	OU = Engineering
	O = Advanced Micro Devices
	L = Santa Clara
	ST = CA
	C = US

Subject Public Key Info	ECDSA on curve P-384
AuthorityKeyIdentifier	The SHA1 of ICA public key
SubjectKeyIdentifier	SHA1 of VCEK public key
Extensions	See Section 3.1. Certificate Extensions and TCB Definitions

[*] *The notValidBefore date is backdated one day prior to the actual issuance date to avoid false certificate verification failures due to out-of-sync system clocks between AMD and the customer.*

3.1 Certificate Extensions and TCB Definitions

Each VCEK certificate contains custom extensions, some of which describe elements that make up the TCB_VERSION structure definition. (See SNP ABI, Section 2.2.) Below are tables showing extensions for different products and versions of the TCB structure.

Notes:

1. The productName extension includes the specific silicon stepping corresponding to the supplied hwID. For example, “Milan-B0,” “Genoa-A0,” etc.
2. Extensions with OIDs prefixed by 1.3.6.1.4.3704.1.3 are elements of the TCB_VERSION structure and are listed in the structure order.
3. Extensions named spl_4, spl_5, etc. are just placeholders for unused bytes of the TCB_VERSION structure and always have the value of 0x00. Numbering on these extensions may not align with their actual positions within the TCB_VERSION structure.
4. For Family 19h processors like Milan and Genoa (Table 10), the hwID is 128 hex characters (64 bytes) long. For Family 1Ah processors (Turin and later) (Table 11), the hwID is 16 hex characters (8 bytes).

Table 10. VCEK Certificate Extensions for Family 19h (structVersion = 0)

OID	Name	ASN.1 Type
1.3.6.1.4.1.3704.1.1	structVersion	INTEGER
1.3.6.1.4.1.3704.1.2	productName	IA5STRING
1.3.6.1.4.1.3704.1.3.1	blSPL	INTEGER
1.3.6.1.4.1.3704.1.3.2	teeSPL	INTEGER
1.3.6.1.4.1.3704.1.3.4	spl_4	INTEGER
1.3.6.1.4.1.3704.1.3.5	spl_5	INTEGER
1.3.6.1.4.1.3704.1.3.6	spl_6	INTEGER
1.3.6.1.4.1.3704.1.3.7	spl_7	INTEGER
1.3.6.1.4.1.3704.1.3.3	snpSPL	INTEGER
1.3.6.1.4.1.3704.1.3.8	ucodeSPL	INTEGER
1.3.6.1.4.1.3704.1.4	hwID*	OCTET

* hwID is 64 octets long on Milan, Genoa, and Siena.

Table 11. VCEK Certificate Extensions for Family 1Ah (Turin) (structVersion = 1)

OID	Name	ASN.1 Type
1.3.6.1.4.1.3704.1.1	structVersion	INTEGER
1.3.6.1.4.1.3704.1.2	productName	IA5STRING
1.3.6.1.4.1.3704.1.3.9	fmcSPL	INTEGER
1.3.6.1.4.1.3704.1.3.1	blSPL	INTEGER
1.3.6.1.4.1.3704.1.3.2	teeSPL	INTEGER
1.3.6.1.4.1.3704.1.3.3	snpSPL	INTEGER
1.3.6.1.4.1.3704.1.3.5	spl_5	INTEGER
1.3.6.1.4.1.3704.1.3.6	spl_6	INTEGER
1.3.6.1.4.1.3704.1.3.7	spl_7	INTEGER
1.3.6.1.4.1.3704.1.3.8	ucodeSPL	INTEGER
1.3.6.1.4.1.3704.1.4	hwID*	OCTET

* hwID is 8 octets long on Turin and beyond.

Chapter 4 VCEK Certificate Access Methods

The AMD Key Distribution System (KDS) provides an HTTP interface (using TLS 1.2) for retrieving VCEK certificate information. All URLs are hosted at *https://kdsintf.amd.com*.

Table 12. VCEK KDS Interface Summary

URI	Description
vcek/v1/{product_name}/{hwid}?{params}	Returns the VCEK certificate for the specified device and SPL values.
vcek/v1/{product_name}/cert_chain	Returns the ARK and ASK for the named product. Certificates are sent in PEM format.
vcek/v1/{product_name}/crl	Returns list of revoked certificates as per RFC 5280. CRL is sent in DER format.

When accessing these URIs, please consider the following:

- The API may impose rate limits on requests, resulting in an Error 429 Too Many Requests. Clients should honor the provided Retry-After value. This typically happens if identical requests are received within 10 seconds of each other.
- Unsupported URLs and nonexistent device IDs will return Error 404 unless otherwise noted in the URI descriptions below.
- In general, expect responses from the KDS to contain the following HTTP headers:
  - content-length
  - content-type
  - content-disposition
  - cache-control
- For valid values of product_name, refer to Section 1.5.

4.1 Get VCEK Certificate for Specified TCB

Table 13. Get VCEK Certificate

<table>
<tr><td><b>URI</b></td><td>vcek/v1/{product_name}/{hwID}?{parameters}
[Note: hwID to be specified in hexadecimal and is either 128 or 16 characters long depending on the product. See Section 3.1]</td></tr>
<tr><td><b>Request Type</b></td><td>GET</td></tr>
<tr><td><b>Cache-control</b></td><td>-</td></tr>
<tr><td><b>URL parameters</b></td><td>
<table>
<tr><th>Parameters for Milan, Genoa, Siena</th><th>Parameters for Turin</th></tr>
<tr><td>blSPL=n</td><td>fmcSPL=n</td></tr>
<tr><td>teeSPL=n</td><td>blSPL=n</td></tr>
<tr><td>snpSPL=n</td><td>teeSPL=n</td></tr>
<tr><td>ucodeSPL=n</td><td>snpSPL=n</td></tr>
<tr><td></td><td>ucodeSPL=n</td></tr>
</table>
[Notes:
- Omitted parameters are assumed to have a value of zero.
- Valid values for ucodeSPL are 0-255, decimal format.
- Valid values for all other parameters are 0-127, decimal format.
- Parameters are separated with “&” and not order dependent.</td></tr>
<tr><td><b>Data parameters</b></td><td>n/a</td></tr>
<tr><td><b>Result</b></td><td>Returns the VCEK Certificate corresponding to the TCB with the specified SPL values. Unspecified SPL values are assumed to be zero.</td></tr>
<tr><td><b>Errors</b></td><td>429 Too Many Requests: If the request rate is exceeded.
400 Bad Request:
- If unexpected or incorrectly sized parameters are encountered in the URI.
- If any specified SPL value exceeds the latest SPL for that entity.</td></tr>
</table>

4.2 Get Certificate Chain

Table 14. Get Certificate Chain

URI	vcek/v1/{product_name}/cert_chain
Request Type	GET
Cache-control	-
URL parameters	n/a
Data parameters	n/a
Result	Returns the ASK and ARK certificates (PEM format, in that order) for the specified product name.
Errors	400 Bad Request: - If unexpected or incorrectly sized parameters are encountered in the URI.

4.3 Get Certificate Revocation List (CRL)

Table 15. Get Certificate Revocation List

URI	vcek/v1/{product_name}/crl
Request Type	GET
Cache-control	-
URL parameters	n/a
Data parameters	n/a
Result	Returns the DER-formatted certificate revocation list for the named product, including the certificate chain, as per section 5 of RFC 5280.
Errors	400 Bad Request: - If unexpected or incorrectly sized parameters are encountered in the URI.

Chapter 5 Integration Details

This section describes ways the VCEK service is designed to ease customer integration.

5.1 Pre-Fetching Certificates for New TCB Values

The SPL values for each firmware make up the TCB. If security vulnerabilities are discovered, firmware updates are released, and the minimum SPL is increased. These updates are typically communicated before the actual release of updated firmware or microcode. The ability to upgrade security firmware without waiting for new VCEK certificates to be requested and installed is desirable.

To support this, the VCEK certificate service allows certificate requests to contain any SPL value within its legal range. (See Section 4.1 for details of allowed values.) This permits customers to pre-fetch and locally cache certificates with SPL values greater than currently released firmware, thereby allowing more seamless upgrades to future firmware versions.