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

Publication # **57230** Revision: **0.50**	
Issue Date: **October 2021**	

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

Contents

List of Tables

Revision History

Date	Revision	Description
October 2021	0.50	Initial public release.

Chapter 1 Introduction

1.1 Purpose and Scope

This document describes the contents of the VCEK certificate and the KDS interface used to retrieve certificate information.

VCEK certificates are used within the context of AMD SEV-SNP technology, the details of which are not described here. For SEV-SNP information, please refer to the specification listed in the References section.

1.2 Intended Audience

The intended audience of this document is software developers supporting virtualized host environments that will employ SEV-SNP technology and need to retrieve VCEK certificates for their secure 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	SEV Secure Nested Paging Firmware ABI Specification. *https://www.amd.com/system/files/TechDocs/56860.pdf*
55766	Secure Encrypted Virtualization API Version 0.24 *https://www.amd.com/system/files/TechDocs/55766_SEV-KM_API_Specification.pdf*

1.4 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 instruction on the processor and comparing the Family/Model/Stepping (FMS) information (see Table 2. Processor Version Information Definition and Table 3. Values for product_name.

Table 2. 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 3. Values for product_name

Extended Family ID	Family ID	Extended Model ID	product_name
Ah	Fh	0h	“Milan”

1.5 Glossary

Term	Definition
ARB	**Anti-Rollback**. Methods used to prevent installation of older firmware/software which contains an exploitable vulnerability.
KDS	**Key Distribution System.** The system of HSMs and supporting hardware/software that manages various cryptographic resources including VCEK certificate generation.
SEV	**Secure Encrypted Virtualization.** An AMD technology to encrypt the memory of a virtual machine using a unique key.
SNP	**Secure Nested Paging.** An extension of SEV features that strengthens memory encryption protections which use newer hardware-based security.
SPL	**Security Patch Level**. Used interchangeably with SVN.
SVN	**Security Version Number**. A version number used to prevent Rollback attacks. Software updates with an SVN lower than the currently installed SVN are not permitted.
TCB	**Trusted Compute Base**. A “TCB version” refers to a specific combination of versions of firmware entities that are part of the TCB (for example, bootloader firmware, SNP firmware, CPU microcode, etc).
VCEK	**Versioned Chip Endorsement Key**. A private ECDSA key which is unique to each AMD chip running a specific TCB version.

Chapter 2 VCEK Certificate Trust Chain

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

2.1 VCEK Signing Keys

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

Key	Abbr.	Algorithm	Usage
AMD Root Key	ARK	RSA 4096	Product-specific AMD Root of Trust. Signs the ASK
AMD SEV Signing Key	ASK	RSA 4096	Signs the VCEK

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

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

Table 4. 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 5. 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.

The following table describes the fields of the VCEK certificate.

<table>
<tr><td><b>Version</b></td><td>V3</td></tr>
<tr><td><b>Serial Number</b></td><td>Zero</td></tr>
<tr><td><b>Issuer</b></td><td>[Subject of ASK certificate]</td></tr>
<tr><td><b>Signature Algorithm</b></td><td>RSASSA-PSS</td></tr>
<tr><td><b>Signature hash algorithm</b></td><td>sha384</td></tr>
<tr><td><b>Validity</b></td><td>Not Before: 0Z
Not After: Seven years after date of issuance</td></tr>
<tr><td><b>Subject</b></td><td>CN = SEV-VCEK
OU = Engineering
O = Advanced Micro Devices
L = Santa Clara
ST = CA
C = US</td></tr>
<tr><td><b>Subject Public Key Info</b></td><td>ECDSA on curve P-384</td></tr>
<tr><td><b>Issuer Unique ID</b></td><td>Not present</td></tr>
<tr><td><b>Subject Unique ID</b></td><td>Not present</td></tr>
<tr><td><b>Extensions</b></td><td>
<table>
<tr><th>OID</th><th>Name</th><th>TAG</th></tr>
<tr><td>1.3.6.1.4.1.3704.1.1</td><td>structVersion</td><td>INTEGER</td></tr>
<tr><td>1.3.6.1.4.1.3704.1.2</td><td>productName[1]</td><td>IA5STRING</td></tr>
<tr><td>1.3.6.1.4.1.3704.1.3.1</td><td>blSPL</td><td>INTEGER</td></tr>
<tr><td>1.3.6.1.4.1.3704.1.3.2</td><td>teeSPL</td><td>INTEGER</td></tr>
<tr><td>1.3.6.1.4.1.3704.1.3.3</td><td>snpSPL</td><td>INTEGER</td></tr>
<tr><td>1.3.6.1.4.1.3704.1.3.4</td><td>spl_4</td><td>INTEGER</td></tr>
<tr><td>1.3.6.1.4.1.3704.1.3.5</td><td>spl_5</td><td>INTEGER</td></tr>
<tr><td>1.3.6.1.4.1.3704.1.3.6</td><td>spl_6</td><td>INTEGER</td></tr>
<tr><td>1.3.6.1.4.1.3704.1.3.7</td><td>spl_7</td><td>INTEGER</td></tr>
<tr><td>1.3.6.1.4.1.3704.1.3.8</td><td>ucodeSPL</td><td>INTEGER</td></tr>
<tr><td>1.3.6.1.4.1.3704.1.4</td><td>hwID</td><td>OCTET</td></tr>
</table>
[1] The productName in this OID includes the specific silicon stepping corresponding to the supplied hwID. For example, “Milan-B0”</td></tr>
</table>

3.1 Mapping TCB Version Numbers to SNP Firmware

The TCB_VERSION string (see SNP ABI, section 2.2) can be constructed from the contents of the VCEK certificate as described in Table 6. TCB_Version to OID Mapping.

Table 6. TCB_Version to OID Mapping

TCB_VERSION Structure		VCEK Certificate	
Bits	**Field**	**OID**	**Name**
63:56	Microcode	1.3.6.1.4.1.3704.1.3.8	ucodeSPL
55:48	SNP	1.3.6.1.4.1.3704.1.3.3	snpSPL
47:40	Reserved	1.3.6.1.4.1.3704.1.3.7	spl_7
39:32	Reserved	1.3.6.1.4.1.3704.1.3.6	spl_6
31:24	Reserved	1.3.6.1.4.1.3704.1.3.5	spl_5
23:16	Reserved	1.3.6.1.4.1.3704.1.3.4	spl_4
15:8	TEE	1.3.6.1.4.1.3704.1.3.2	teeSPL
7:0	BOOT_LOADER	1.3.6.1.4.1.3704.1.3.1	blSPL

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 7. VCEK KDS Interface Summary

URI	Description
vcek/v1/{product_name}/{hwid}?{tcb parameter list}	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.
- Unsupported URLs 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 1.4

4.1 Get VCEK Certificate for Specified TCB

URI	vcek/v1/{product_name}/{hwID}?{parameters} [Note: hwID to be specified in hexadecimal]
Request Type	GET
Cache-control	-
URL parameters	blSPL=nn teeSPL=nn snpSPL=nn ucodeSPL=nn [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.
Data parameters	n/a
Result	Returns the VCEK Certificate corresponding to the TCB with the specified SPL values. Unspecified SPL values are assumed to be zero.
Errors	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.

4.2 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)

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 will permit 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.