AMD

Versioned Loaded Endorsement Key (VLEK) Certificate Definition

Publication #	**58369**	Revision:	**0.10**
Issue Date:	**October 2023**		

Advanced Micro Devices

Contents

List of Tables

Revision History

Date	Revision	Description
August 2023	0.10	• Initial public release

Chapter 1 Introduction

1.1 Purpose and Scope

This document describes contents of the Versioned Loaded Endorsement Key (VLEK) certificate. VLEK 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 users and developers of virtualized host environments that employ AMD's SEV-SNP technology and need to understand the contents of VLEK certificates and how to retrieve certificate authorities to validate them.

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 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.** A key used as the Root CA for VLEK certificates. Each product (e.g., Milan) has its own ARK and Root CA certificate.
ASVK	**AMD SEV-VLEK Key.** A key used as an intermediate CA that signs VLEK certificates. Each product (e.g., Milan) has its own ASVK and ICA certificate.

Term	Definition
CSP	**Cloud Service Provider.** A company/entity that is using the KDS VLEK interface to request certificates and hash sticks.
CSP_ID	**Cloud Service Provider Identifier**. A string used to uniquely identify a cloud service provider. The subject field from the client's TLS certificate is used as the CSP_ID.
KDS	**Key Distribution System.** AMD's system of hardware security modules (HSMs) and supporting hardware/software that manages various cryptographic resources including VLEK 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 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/Boundary**. 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**. An Elliptic Curve Digital Signature Algorithm (ECDSA) key unique to each AMD chip running a specific TCB version.
VLEK	**Versioned Loaded Endorsement Key**. An ECDSA key unique to a specific CSP and TCB version.
VLEK Seed	A 256-bit value unique to each combination of CSP_ID and product, used as the seed to derive a VLEK hash stick.

1.5 Determining the Product Name

The name of the product appears in the ARK, ASVK, and VLEK 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

Extended Family ID	Family ID	Extended Model ID	product_name
Ah	Fh	0h	“Milan”
Ah	Fh	1h	“Genoa”

Chapter 2 VLEK Certificate Trust Chain

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

2.1 Certificate Authorities

The VLEK certificate is rooted through a certificate chain described by Table 5. VLEK Certificate Chain.

Table 5. VLEK Certificate Chain

Key	Abbr.	Key Type	Description
AMD Root Key	ARK	RSA 4096	Product-specific AMD Root of Trust. Signs the ASVK intermediate CA.
AMD SEV-VLEK Key	ASVK	RSA 4096	Product-specific intermediate CA that signs VLEK certificates.

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

2.2 Downloading the CA Certificates and CRL

Certificates for the ARK and ASVK 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/

Port	URI	Method	Description
443	/vlek/v1/{product_name*}/cert_chain	GET	Returns the product-specific CA chain. Certificates are sent in PEM format.
443	/vlek/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 ASVK Certificate Definitions

Table 6. 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) OU = Engineering O = Advanced Micro Devices L = Santa Clara S = CA C = US
Subject Public Key Info	RSA (4096 bits)
CRL Distribution Point	URL=https://kdsintf.amd.com/vlek/v1/{product_name}/crl
Key Usage	Certificate Signing, Off-line CRL Signing, CRL Signing

Table 7. AMD SEV-VLEK Key (ASVK) 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-VLEK OU = Engineering O = Advanced Micro Devices L = Santa Clara S = CA C = US
Subject Public Key Info	RSA (4096 bits)
CRL Distribution Point	URL=https://kdsintf.amd.com/vlek/v1/{product_name}/crl
Key Usage	Certificate Signing

Chapter 3 VLEK Certificate Format

The VLEK 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 8 describes the fields of the VLEK certificate.

Table 8. VLEK Certificate Fields

Version	V3
Serial Number	Zero
Issuer	[Subject of ASVK certificate]
Signature Algorithm	RSASSA-PSS
Signature Hash Algorithm	sha384
Validity	Not before: one day prior to date of issuance[1] Not after: seven years after date of issuance
Subject	CN = SEV-VLEK 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 VLEK public key
Extensions	See Section 3.1. Certificate Extensions and TCB Definitions

Note:

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

3.1 Certificate Extensions and TCB Definitions

Each VLEK 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 the 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 position within the TCB_VERSION structure.

Table 9. VLEK Certificate Extensions for Milan and Genoa (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
1.3.6.1.4.1.3704.1.5	csp_id	IA5STRING