Nuvoton Trusted Platform Module (TPM) Endorsement Key (EK) Certificate Chain

Revision	Date	Author	Comments
1.0	June 15, 2020	Dana Cohen	First release.
1.1	April 11, 2021	Dana Cohen	Added support for new certificates.
1.2	May 26, 2021	Dana Cohen	Fixed certificate 2012 content (Table 2).
1.3	June 14, 2021	Dana Cohen	Fixed certificate 2012 TPM level (TPM1.2 instead of TPM 2.0). Reordered elements in Tables 1 and 2.
1.4	October 4, 2021	Dana Cohen	Added element in Table 1. Added Table 3.
1.5	November 25, 2021	Dana Cohen	Changed certificate headers.
1.6	April 7, 2022	Dana Cohen	Added two new certificates to Table 1.
1.7	June 6, 2022	Dana Cohen	Fixed certificate convention and links
2.0	May 7, 2023	Dana Cohen	Added support for new root and intermediate certificates.
2.1	Aug 2, 2023	Dana Cohen	Updated section 3.

Table of Contents

1. General

Introduction

Document Organization

This document contains the following sections:

1. General information about this document
2. Nuvoton TPM Certificate Chain
3. Required Steps to Read and Verify EK Certificates from Nuvoton TPMs

Purpose

The purpose of this document is to enable a Nuvoton TPM user to verify the genuineness of TPM on the system (i.e. was manufactured and signed by Nuvoton).

This document describes the certificate chain starting from the Endorsement Key (EK) certificates of the Nuvoton Trusted Platform Module (TPM), up to the Root.

The Nuvoton TPM endorsement key (EK) certificates are provided in X.509 format.

References

In this document, “TPM” refers to the Nuvoton NPCT7/6/5/4xx devices.

Both devices implement all TCG commands and functionality, as defined in the following TCG specifications:

[TPM2.0] *Trusted Platform Module Library Specification, Family “2.0”, Level 00, Revision 01.59*

and

Trusted Platform Module Library Specification, Family "2.0", Level 00, Revision 01.38
and
Trusted Platform Module Library Specification, Family “2.0”, Level 00, Revision 01.16
https://trustedcomputinggroup.org/resource/tpm-library-specification/

[TPM1.2] *TPM Main Specification Level 2 Version 1.2, Revision 116*

https://trustedcomputinggroup.org/resource/tpm-main-specification

[CRED2.0] *TCG EK Credential Profile for TPM Family 2.0; Level 0 Specification Version 2.4 Revision 3*

https://trustedcomputinggroup.org/resource/tcg-ek-credential-profile-for-tpm-family-2-0

[CRED1.2] *TCG Credential Profiles for TPM Family 1.2; Level 2 Specification Version 1.2 Revision 8*

https://www.trustedcomputinggroup.org/wp-content/uploads/Credential_Profiles_V1.2_Level2_Revision8.pdf

2. Nuvoton TPM Root EK Certificates

Nuvoton pre-installs EK certificates in its TPM products during manufacturing.

NPCT7xx EK certificates are signed by Nuvoton Intermediate CAs whose certificates are signed by a self-signed Nuvoton Root CA.

NPCT4xx/5xx/6xx & 7xx (Legacy) EK certificates are signed directly by self-signed Nuvoton Root CAs.

The following tables describe the Nuvoton TPM Intermediate and Root CAs.

Table 1. NPCT7xx Intermediate CAs

NPCTxxx ECC384 LeafCA 012110 (signing TPM2.0 EK certificates)	
AIA	https://www.nuvoton.com/security/NTC-TPM-EK-Cert/NPCTxxxECC384LeafCA012110.cer
Name Hash	16 36 81 31 68 cb f0 71 0b b7 eb 6f 5c 66 21 35 6d e2 1e 7c
SKI	b6 ea a1 1f 20 1f f7 4e d4 f2 51 0e 15 bf 2e 38 84 dc 40 55
Certificate Issuer Identifier	ad 93 c8 4a c4 88 c6 1f 53 b0 ca de c0 5e ee 9f e3 3f 08 cd
Thumbprint	e0 c1 51 21 59 88 f3 89 08 45 81 bf 45 af b8 f1 52 c0 d6 23
NPCTxxx ECC384 LeafCA 012111 (signing TPM2.0 EK certificates)	
AIA	https://www.nuvoton.com/security/NTC-TPM-EK-Cert/NPCTxxxECC384LeafCA012111.cer
Name Hash	16 36 81 31 68 cb f0 71 0b b7 eb 6f 5c 66 21 35 6d e2 1e 7c
SKI	b5 57 7f ee 83 30 16 1b b2 fe 6d ba b6 6b f2 bc 37 f5 1a 7a
Certificate Issuer Identifier	ad 93 c8 4a c4 88 c6 1f 53 b0 ca de c0 5e ee 9f e3 3f 08 cd
Thumbprint	97 b6 7d 12 d8 f6 ae 14 24 58 48 45 93 da 3b 7a 91 d6 46 74
NPCTxxx ECC384 LeafCA 022110 (signing TPM2.0 EK certificates)	
AIA	https://www.nuvoton.com/security/NTC-TPM-EK-Cert/NPCTxxxECC384LeafCA022110.cer
Name Hash	16 36 81 31 68 cb f0 71 0b b7 eb 6f 5c 66 21 35 6d e2 1e 7c
SKI	61 d1 9d a2 2b 4f 88 fe e2 ae c4 11 46 de e8 67 15 d1 ca 15
Certificate Issuer Identifier	ad 93 c8 4a c4 88 c6 1f 53 b0 ca de c0 5e ee 9f e3 3f 08 cd
Thumbprint	d1 2e c7 ab a8 53 12 4c d8 75 be 9f eb 0a 21 20 8a 97 26 d8

NPCTxxx ECC384 LeafCA 022111 (signing TPM2.0 EK certificates)	
AIA	https://www.nuvoton.com/security/NTC-TPM-EK-Cert/NPCTxxxECC384LeafCA022111.cer
Name Hash	16 36 81 31 68 cb f0 71 0b b7 eb 6f 5c 66 21 35 6d e2 1e 7c
SKI	32 bd cc 82 a7 37 cc 5a 80 5a cb bb 19 82 5a 62 d4 fb 99 f5
Certificate Issuer Identifier	ad 93 c8 4a c4 88 c6 1f 53 b0 ca de c0 5e ee 9f e3 3f 08 cd
Thumbprint	97 b6 7d 12 d8 f6 ae 14 24 58 48 45 93 da 3b 7a 91 d6 46 74

Table 2. NPCT7xx Root CA

NPCTxxx ECC521 Root CA (signing Intermediate CA)	
AIA	https://www.nuvoton.com/security/NTC-TPM-EK-Cert/NPCTxxxECC521RootCA.cer
Name Hash	16 36 81 31 68 cb f0 71 0b b7 eb 6f 5c 66 21 35 6d e2 1e 7c
SKI	ad 93 c8 4a c4 88 c6 1f 53 b0 ca de c0 5e ee 9f e3 3f 08cd
Certificate Issuer Identifier	ad 93 c8 4a c4 88 c6 1f 53 b0 ca de c0 5e ee 9f e3 3f 08cd
Thumbprint	7c 7b 3c 8a 46 5e 67 d2 8f 4d b0 f3 5c e1 20 c4 bb 4a ac cc

Table 3. Legacy NPCT7xx Root CAs

Nuvoton TPM Root CA 2210 (signing TPM2.0 EK certificates)	
AIA	https://www.nuvoton.com/security/NTC-TPM-EK-Cert/NuvotonTPMRootCA2210.cer
Name Hash	d3 9c b2 97 0f 47 5b c0 30 f0 98 7c 52 15 41 eb 7c cc 8e 17
SKI	66 7d 15 46 65 ca c0 1f 70 cb 40 d8 db 33 59 4c 90 b4 d9 11
Certificate Issuer Identifier	66 7d 15 46 65 ca c0 1f 70 cb 40 d8 db 33 59 4c 90 b4 d9 11
Thumbprint	4a d6 dd bd 52 52 2c 52 1c bf 92 99 c4 46 26 3f 34 81 a6 7a
Nuvoton TPM Root CA 2211 (signing TPM2.0 EK certificates)	
AIA	https://www.nuvoton.com/security/NTC-TPM-EK-Cert/NuvotonTPMRootCA2211.cer
Name Hash	a4 1f a3 5a b9 33 a1 46 11 4f aa 51 46 e2 94 3f e2 30 a0 33
SKI	72 b0 3d 71 22 81 95 34 63 bc 72 60 98 ea 3b c2 f3 b1 3f a6
Certificate Issuer Identifier	72 b0 3d 71 22 81 95 34 63 bc 72 60 98 ea 3b c2 f3 b1 3f a6
Thumbprint	5e 74 87 90 69 4f 6a 7f 6e ab af 70 15 26 86 3c dd fe 6d ac
Nuvoton TPM Root CA 1111 (signing TPM2.0 EK certificates)	
AIA	https://www.nuvoton.com/security/NTC-TPM-EK-Cert/Nuvoton TPM Root CA 1111.cer
Name Hash	c0 a9 74 56 30 89 e7 2b 0e cb 63 0b 10 39 f7 27 65 ad 09 6e
SKI	88 2f 04 7b 87 12 1c f9 88 5f 31 16 0b c7 bb 55 86 af 47 1b
Certificate Issuer Identifier	88 2f 04 7b 87 12 1c f9 88 5f 31 16 0b c7 bb 55 86 af 47 1b
Thumbprint	48 65 2a 31 b9 d2 66 08 4e 2a e9 82 d8 b6 73 26 d6 6c 73 72
Nuvoton TPM Root CA 2111 (signing TPM2.0 EK certificates)	
AIA	https://www.nuvoton.com/security/NTC-TPM-EK-Cert/Nuvoton TPM Root CA 2111.cer
Name Hash	7c 09 52 49 5c e5 99 43 1b 70 20 c7 fe 39 06 af a6 d8 2b 58
SKI	23 f4 e2 2a d3 be 37 4a 44 97 72 95 4a a2 83 ae d7 52 57 2e
Certificate Issuer Identifier	23 f4 e2 2a d3 be 37 4a 44 97 72 95 4a a2 83 ae d7 52 57 2e
Thumbprint	a3 43 0d 4e 2f 07 55 61 96 5a e6 ed 32 c9 1a 3d 73 22 c4 2b

Nuvoton TPM Root CA 2112 (signing TPM2.0 EK certificates)	
AIA	https://www.nuvoton.com/security/NTC-TPM-EK-Cert/Nuvoton TPM Root CA 2112.cer
Name Hash	76 81 00 12 40 34 a9 c3 a0 97 4b 75 30 bd c8 7e 80 8e d8 2f
SKI	e4 a8 66 6f 8f 4c 6d 9c 39 32 a9 48 84 77 80 a6 81 0c 42 13
Certificate Issuer Identifier	e4 a8 66 6f 8f 4c 6d 9c 39 32 a9 48 84 77 80 a6 81 0c 42 13
Thumbprint	58 9a 6b d9 ee 96 3b ec e2 06 58 d1 4a 24 0f 7b 4b 72 40 33
Nuvoton TPM Root CA 1210 (signing TPM2.0 EK certificates)	
AIA	https://www.nuvoton.com/security/NTC-TPM-EK-Cert/NuvotonTPMRootCA1210.cer
Name Hash	5d 1e a5 8b 00 11 16 35 48 b2 68 2f 83 39 e7 b4 c1 04 f9 7a
SKI	e1 51 b0 ab 06 bf f7 5b 07 4e 5b 6a a8 34 e2 da 2f ba 83 83
Certificate Issuer Identifier	e1 51 b0 ab 06 bf f7 5b 07 4e 5b 6a a8 34 e2 da 2f ba 83 83
Thumbprint	86 a9 9e 10 f6 b1 1e 41 bd 19 d8 ef 79 db c9 5a f4 d3 c3 ed
Nuvoton TPM Root CA 1014 (signing TPM1.2 EK certificates)	
AIA	https://www.nuvoton.com/security/NTC-TPM-EK-Cert/Nuvoton TPM Root CA 1014.cer
Name Hash	2f 24 72 c1 18 67 09 41 44 8a fb 0e 01 7e a7 5a 83 22 c2 1a
SKI	a9 d9 47 f3 f9 81 72 ee b6 dc c5 ed 60 9a 00 de 7c 06 9c b0
Certificate Issuer Identifier	a9 d9 47 f3 f9 81 72 ee b6 dc c5 ed 60 9a 00 de 7c 06 9c b0
Thumbprint	fb f7 1e ad 86 ea 64 bf 49 95 0c 33 16 26 9d bf 40 ff e8 71
Nuvoton TPM Root CA 2011 (signing TPM1.2 EK certificates)	
AIA	https://www.nuvoton.com/security/NTC-TPM-EK-Cert/Nuvoton TPM Root CA 2011.cer
Name Hash	82 f5 47 a3 bd aa 3a 63 44 b8 dd cf 8b a8 43 85 92 8e 03 9f
SKI	a5 2c b6 47 e0 90 9b da 2e 7f 7d 91 3f 62 d8 8b 13 89 e2 c6
Certificate Issuer Identifier	a5 2c b6 47 e0 90 9b da 2e 7f 7d 91 3f 62 d8 8b 13 89 e2 c6
Thumbprint	a2 88 69 b5 3d d8 cc a3 52 be d8 d5 2d 55 32 64 d4 cd 40 cf
Nuvoton TPM Root CA 2012 (signing TPM1.2 EK certificates)	
AIA	https://www.nuvoton.com/security/NTC-TPM-EK-Cert/Nuvoton TPM Root CA 2012.cer
Name Hash	8e 64 9b 82 98 1a 16 44 8c 89 bf da 69 3e d0 18 52 2a b0 31
SKI	56 87 37 b0 ec 39 d0 b7 79 c3 dc 7e 81 c1 0f ad 8f 60 a1 59
Certificate Issuer Identifier	56 87 37 b0 ec 39 d0 b7 79 c3 dc 7e 81 c1 0f ad 8f 60 a1 59
Thumbprint	bd 0b 5a 46 e3 7c ce 7f 78 e6 53 81 4a f6 a4 12 b5 3d 73 95

Table 4. NPCT65x Root CAs

Nuvoton TPM Root CA 1110 (signing TPM2.0 EK certificates)	
AIA	https://www.nuvoton.com/security/NTC-TPM-EK-Cert/Nuvoton TPM Root CA 1110.cer
Name Hash	3e 6c 3b 35 ef 14 4b 0a 76 cd cf a4 08 0b 8b 7b ca 3c c8 ee
SKI	15 91 d4 b6 ea f9 8d 01 04 86 4b 69 03 a4 8d d0 02 60 77 d3
Certificate Issuer Identifier	15 91 d4 b6 ea f9 8d 01 04 86 4b 69 03 a4 8d d0 02 60 77 d3
Thumbprint	65 5e 44 5e 96 54 5c f3 e4 84 82 94 9b 35 a7 ce b3 46 58 cc
Nuvoton TPM Root CA 2110 (signing TPM2.0 EK certificates)	
AIA	https://www.nuvoton.com/security/NTC-TPM-EK-Cert/Nuvoton TPM Root CA 2110.cer
Name Hash	d6 59 bc f0 af ff 22 84 ae 8a c2 74 c6 d9 12 15 ae d2 b6 2f
SKI	9f bb 79 aa 0f 52 62 78 be d1 50 92 9a 71 71 e9 6a 35 be f7
Certificate Issuer Identifier	9f bb 79 aa 0f 52 62 78 be d1 50 92 9a 71 71 e9 6a 35 be f7
Thumbprint	4c 62 38 50 16 d6 19 cd 03 cb 68 b1 67 57 2f 6a d6 8e 37 de
Nuvoton TPM Root CA 1012 (signing TPM1.2 EK certificates)	
AIA	https://www.nuvoton.com/security/NTC-TPM-EK-Cert/NTC_TPM_EK_Root_CA_ARSUF_01.cer
Name Hash	a0 74 a1 27 1d df 51 5f 97 b1 f4 b9 d4 4f e2 55 d7 64 45 01
Certificate Subject Identifier	77 0e 97 4a ca f0 db 9a e6 7e 7b 6f 5d 41 0f 9a ce 2f ad 65
Certificate Issuer Identifier	77 0e 97 4a ca f0 db 9a e6 7e 7b 6f 5d 41 0f 9a ce 2f ad 65
Thumbprint	4d b7 58 57 3a 43 68 48 10 26 8a ab 8f 1b 5a 77 b6 6d ab 15
Nuvoton TPM Root CA 1013 (signing TPM1.2 EK certificates)	
AIA	https://www.nuvoton.com/security/NTC-TPM-EK-Cert/Nuvoton TPM Root CA 1013.cer
Name Hash	91 eb bb 7c 51 fa 7f 78 aa 3d 44 d3 42 5b 1d 5d 23 97 5c af
SKI	a0 d7 37 29 0e 16 cf 2a e2 be e7 10 0c f5 6b 2f 04 c5 f0 43
Certificate Issuer Identifier	a0 d7 37 29 0e 16 cf 2a e2 be e7 10 0c f5 6b 2f 04 c5 f0 43
Thumbprint	97 58 d2 63 78 64 d4 fa df bb 87 e6 ed b8 c1 2c 5a d5 80 d7

Nuvoton TPM Root CA 2010 (signing TPM1.2 EK certificates)	
AIA	https://www.nuvoton.com/security/NTC-TPM-EK-Cert/Nuvoton TPM Root CA 2010.cer
Name Hash	bc d3 c5 03 d3 9e 51 b0 c5 04 89 e9 22 8e 98 4a 7e 63 e3 03
SKI	08 30 0f 43 a8 f4 b8 c8 e6 24 a4 f7 06 0c f5 9e 74 50 15 e7
Certificate Issuer Identifier	08 30 0f 43 a8 f4 b8 c8 e6 24 a4 f7 06 0c f5 9e 74 50 15 e7
Thumbprint	ee 07 22 51 f2 35 95 99 c4 ae 99 33 82 4a 54 04 3a c6 1b ff

Table 5. NPCT4/5xx Root CAs

Nuvoton TPM Root CA 1010 (signing TPM1.2 EK certificates)	
AIA	https://www.nuvoton.com/security/NTC-TPM-EK-Cert/NTC TPM EK Root CA 01.cer
Name Hash	a0 74 a1 27 1d df 51 5f 97 b1 f4 b9 d4 4f e2 55 d7 64 45 01
Thumbprint	6e 20 a1 30 52 e1 7e 85 11 87 a1 61 50 41 ce 7b aa 2a 16 66
Nuvoton TPM Root CA 1011 (signing TPM1.2 EK certificates)	
AIA	https://www.nuvoton.com/security/NTC-TPM-EK-Cert/NTC TPM EK Root CA 02.cer
Name Hash	19 bc c8 bf 66 e8 eb 35 75 c1 e8 3a db 8d 4e 16 12 b5 6b 0f
Thumbprint	62 7b 0b 0c 54 5e 27 ba 44 09 a7 91 ca 37 9d 49 5f 47 d8 ff

3. Required Steps for Reading and Verifying the EK Certificate from the Nuvoton TPM

To read an EK certificate from a TPM and verify that it is genuine:

- For TPM2.0: Refer to [CRED2.0] section 2.2.1.9 “Read EK certificates and create the associated EKs”.
- In 5b, the reference to “certificate” assumes the Intermediate CA certificate. For legacy, the reference assumes the self-signed Root CA certificate.

- For TPM1.2: Nuvoton TPM products have pre-installed EKs and EK certificates stored in the `TCG_PCCLIENT_STORED_CERT` structure, with `certType` set to `TCG_FULL_CERT` (i.e., the cert field is `TCG_FULL_CERT` structure).
  EK certificates are stored in NV storage at index `TPM_NV_INDEX_EKCert` (100F000h).
  For structure definitions refer to [TPM1.2] part 2.

Nuvoton provides comprehensive service and support.
For product information and technical assistance, contact the nearest Nuvoton center.

Important Notice

Nuvoton products are not designed, intended, authorized or warranted for use as components in systems or equipment intended for surgical implantation, atomic energy control instruments, airplane or spaceship instruments, transportation instruments, traffic signal instruments, combustion control instruments, or for other applications intended to support or sustain life. Furthermore, Nuvoton products are not intended for applications wherein failure of Nuvoton products could result or lead to a situation wherein personal injury, death or severe property or environmental damage could occur.

Nuvoton customers using or selling these products for use in such applications do so at their own risk and agree to fully indemnify Nuvoton for any damages resulting from such improper use or sales.

CONTACT INFORMATION

For Nuvoton Sales Offices in your region, visit us at:

https://www.nuvoton.com/buy/worldwide-sales-offices/

For Cloud Computing Product Line information, contact:

CloudComputing@nuvoton.com

www.nuvoton.com