ST33KTPM-IDevID - Provisioning profile ST1 description

Introduction

This application note describes the ST33KTPM-IDevID based on the ST1 provisioning profile that is used to configure ST33KTPM (ST33KTPM2I, ST33KTPM2X) devices. For further product descriptions such as package and characteristics, refer to the respective datasheets.

The ST1 profile is based on the Trusted Computing Group's (TCG) TPM 2.0 Keys for Device Identity and Attestation v1.10 specification and provides an Initial Attestation Key-pair (IAK), an Initial Device ID (IDevID) key-pair and associated leaf certificates. The IDevID key and certificate are compatible with cloud authentication systems, such as AWS® IoT and Microsoft Azure®.

The ST33KTPM-IDevID features:

- Two NIST P-384 (secp384r1) key pairs and associated x.509 certificate signed by an ST certificate authority (CA).
  - The "Subject::Common Name" field of the leaf certificate contains the unique serial number (CPSN) of the ST33KTPM-IDevID.
  - The certificates are stored permanently in the ST33KTPM-IDevID non-volatile memory.
- Each key pair (IAK/IDevID) has different capabilities, and the use of their private key is controlled by a diversified password or a specific authentication value (*authValue*).
  - An attestation key pair (IAK), with restricted signing TPM attributes to support attestation use cases.
  - An authentication key pair (IDevID) which can be used for device identification use cases, typically authentication for remote server and cloud-based solutions.
- Each ECC NIST P-384 key pair is generated by the ST33KTPM-IDevID. The public key is embedded in the CA-signed leaf certificate, while the private key is securely stored within the ST33KTPM device.

A bundle file containing the device leaf certificates is provided for individual reels of devices.

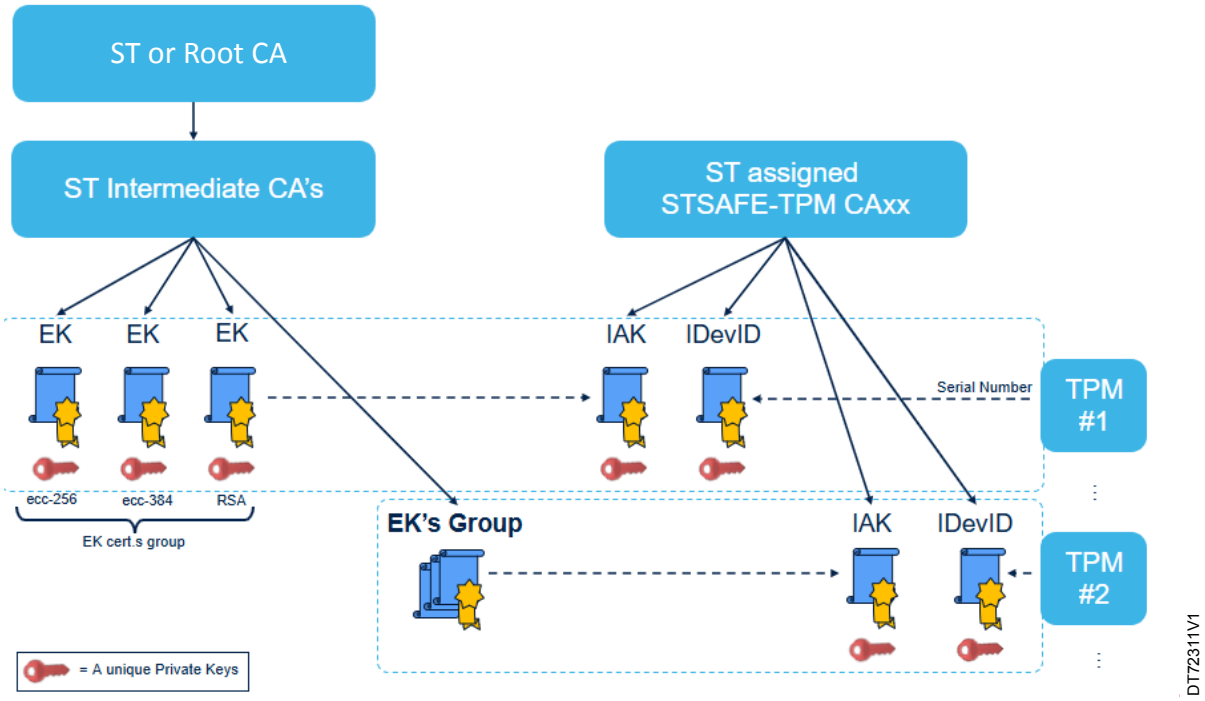
This facilitates:

- Allows the certificates to be loaded into the cloud system before getting physical access to the provisioned TPMs
- Keeping track of TPM devices shipped and providing a means to revoke certificates should there be any supply chain issue

1 Public key infrastructure

Figure 1 illustrates the public key infrastructure (PKI) used in the provisioning of the ST33KTPM-IDevID with ST1 profile.

Figure 1. Public key infrastructure



It defines two hierarchies:

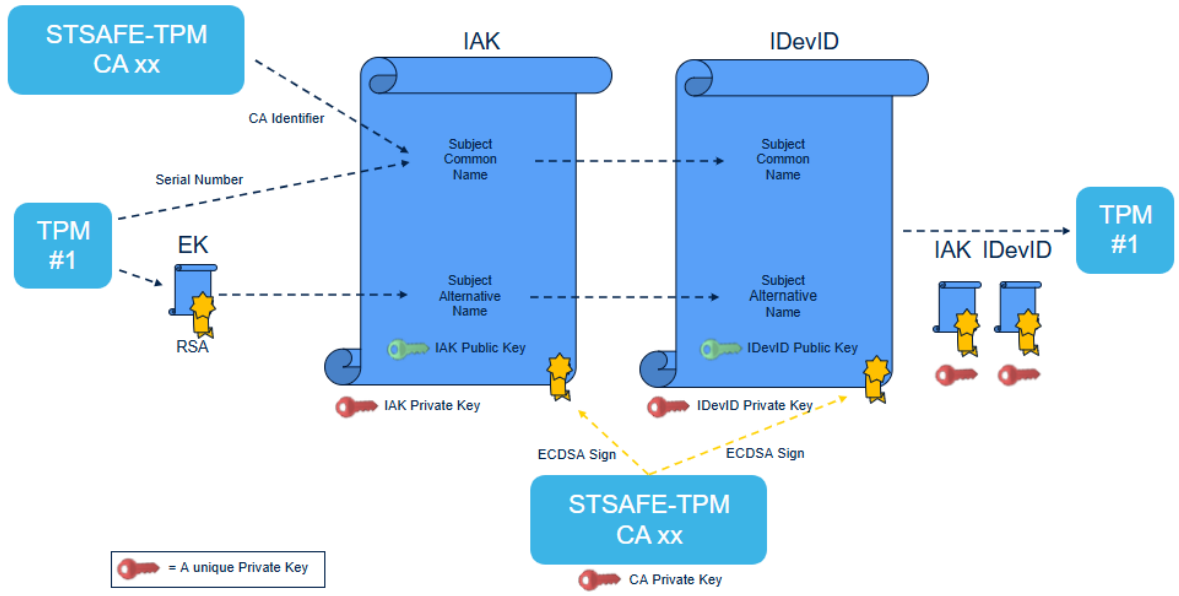
1. The endorsement keys (EK) key-pairs and associated certificates
   - 3-level hierarchy
     a. ST CA Root CA
     b. Three ST Intermediate CA's one for each algorithm (RSA-2048, EC-256, EC-384) defined for the product family, with a key-pair correspondingly
     c. The EK key-pairs, one for each algorithm type (RSA-2048, EC-256, EC-384), and their associated certificates (x.509) as defined in TCG Endorsement Key Credential Profile specification ([TCG EK Cre Profile TPM 2.3])
2. The IAK and IDevID ECC NIST P-384 key-pairs and associated certificates
   - 2-level hierarchy
     a. ST STSAFE-TPM CA (ECC-384) key-pair
     b. The IAK key-pair and associated certificate (x.509)
     c. The IDevID key-pair and associated certificate (x.509)

2 Leaf certificates

The STSAFE-TPM CA signs X.509 leaf certificates.

The IAK and IDevID certificates include unique information that links them to a specific TPM device. This binding, as illustrated in Figure 2, is derived from the EK certificate and the TPM unique serial number (CPSN).

Figure 2. Leaf certificate infrastructure



3 ST Certificate Authority Certificate

The ST STSAFE-TPM certificate authority (CA) certificates are based on SHA384/ECDSA NIST P-384 (secp384r1) key signature.

The ST STSAFE-TPM CA (for CA number 0xF0) certificate below can be used to verify the ST1 IAK and IDevID leaf certificates.

Below is the DER format:

```
30 82 01 F0 30 82 01 77 A0 03 02 01 02 02 02 40 F0 30 0A 06 08 2A 86 48 CE 3D 04 03 03 30 48
31 0B 30 09 06 03 55 04 06 13 02 4E 4C 31 1E 30 1C 06 03 55 04 0A 13 15 53 54 4D 69 63 72 6F
65 6C 65 63 74 72 6F 6E 69 63 73 20 6E 76 31 19 30 17 06 03 55 04 03 13 10 53 54 53 41 46 45
2D 54 50 4D 20 43 41 20 46 30 30 20 17 0D 32 35 30 32 30 36 31 31 31 37 31 37 5A 18 0F 39 39
39 39 31 32 33 31 32 33 35 39 35 39 5A 30 48 31 0B 30 09 06 03 55 04 06 13 02 4E 4C 31 1E 30
1C 06 03 55 04 0A 13 15 53 54 4D 69 63 72 6F 65 6C 65 63 74 72 6F 6E 69 63 73 20 6E 76 31 19
30 17 06 03 55 04 03 13 10 53 54 53 41 46 45 2D 54 50 4D 20 43 41 20 46 30 30 76 30 10 06 07
2A 86 48 CE 3D 02 01 06 05 2B 81 04 00 22 03 62 00 04 AB 85 FA 0F 1D 15 3F 39 78 21 21 2A 4C
4E D7 36 65 C0 B6 65 99 5E D5 D8 B9 21 87 67 D5 B2 FF 85 9C E9 70 F5 B7 D2 BE 3C F9 4B 55 08
43 E2 F7 7C 8E 49 50 68 0F A6 12 66 8C 32 4E 64 45 C4 A5 4E 3A 0F AD 4E 82 20 85 12 5E 80 F8
59 30 9E AE DF 8C E8 A7 CA 28 3B DE BC 03 2A A0 42 9C 6F 1E 18 A3 32 30 30 30 0F 06 03 55 1D
13 01 01 FF 04 05 30 03 01 01 FF 30 1D 06 03 55 1D 0E 04 16 04 14 62 86 0D 25 F2 60 20 6B 16
22 0A 3D 4F BE 66 F0 72 2F 72 43 30 0A 06 08 2A 86 48 CE 3D 04 03 03 03 67 00 30 64 02 30 5B
88 6E 08 BB AF 6B 58 18 62 8C 6C 34 A5 EC B5 49 84 98 E5 CA 32 9C D1 03 55 01 9D 0B 40 88 21
87 03 05 4D EA E4 BF 39 CF 5D F1 07 AA 2A 08 FC 02 30 44 D1 B0 64 C5 56 48 8B 13 EA 33 D3 6D
1A B0 6F 1C 39 0A 74 2F B6 9C E8 48 FD 46 BD 0A 07 74 E4 31 EF 2B 30 97 66 80 01 17 28 DD E7
CB E9 FC CF
```

Below if the PEM format:

```
-----BEGIN CERTIFICATE-----
MIIB8DCCAXegAwIBAgICQPAwCgYIKoZIzj0EAwMwSDELMAkGA1UEBhMCTkwxHjAc
BgNVBAoTFVNUTWljcm9lbGVjdHJvbmljcyBudjEZMBcGA1UEAxMQU1RTQUZFLVRQ
TSBDQSBGMDAgFw0yNTAyMDYxMTE3MTdaGA85OTk5MTIzMTIzNTk1OVowSDELMAkG
A1UEBhMCTkwxHjAcBgNVBAoTFVNUTWljcm9lbGVjdHJvbmljcyBudjEZMBcGA1UE
AxMQU1RTQUZFLVRQTSBDQSBGMDB2MBAGByqGSM49AgEGBSuBBAAiA2IABKuF+g8d
FT85eCEhKkxO1zZlwLZlmV7V2Lkhh2fVsv+FnOlw9bfSvjz5S1UIQ+L3fI5JUGgP
phJmjDJOZEXEpU46D61OgiCFEl6A+Fkwnq7fjOinyig73rwDKqBCnG8eGKMyMDAw
DwYDVR0TAQH/BAUwAwEB/zAdBgNVHQ4EFgQUYoYNJfJgIGsWIgo9T75m8HIvckMw
CgYIKoZIzj0EAwMDZwAwZAIwW4huCLuva1gYYoxsNKXstUmEmOXKMpzRA1UBnQtA
iCGHAwVN6uS/Oc9d8QeqKgj8AjBE0bBkxVZIixPqM9NtGrBvHDkKdC+2nOhI/Ua9
Cgd05DHvKzCXZoABFyjd58vp/M8=
-----END CERTIFICATE-----
```

The certificate can also be retrieved from this URL: http://sw-center-st-com.s3.amazonaws.com/STSAFE/stsafetpmca_F0.crt.

3.1 STSAFE-TPM CA self-signed certificate

The X.509 CA certificate for CA number 0xF0:

```
Certificate:
    Data:
        Version: 3 (0x2)
        Serial Number: 16624 (0x40f0)
    Signature Algorithm: ecdsa-with-SHA384
        Issuer: C = NL, O = STMicroelectronics nv, CN = STSAFE-TPM CA F0
        Validity
            Not Before: Feb 6 11:17:17 2025 GMT
            Not After : Dec 31 23:59:59 9999 GMT
        Subject: C = NL, O = STMicroelectronics nv, CN = STSAFE-TPM CA F0
        Subject Public Key Info:
            Public Key Algorithm: id-ecPublicKey
                Public-Key: (384 bit)
                pub:
                    04:ab:85:fa:0f:1d:15:3f:39:78:21:21:2a:4c:4e:
                    d7:36:65:c0:b6:65:99:5e:d5:d8:b9:21:87:67:d5:
                    b2:ff:85:9c:e9:70:f5:b7:d2:be:3c:f9:4b:55:08:
                    43:e2:f7:7c:8e:49:50:68:0f:a6:12:66:8c:32:4e:
                    64:45:c4:a5:4e:3a:0f:ad:4e:82:20:85:12:5e:80:
                    f8:59:30:9e:ae:df:8c:e8:a7:ca:28:3b:de:bc:03:
                    2a:a0:42:9c:6f:1e:18
                ASN1 OID: secp384r1
                NIST CURVE: P-384
        X509v3 extensions:
            X509v3 Basic Constraints: critical
                CA:TRUE
            X509v3 Subject Key Identifier:
                62:86:0D:25:F2:60:20:6B:16:22:0A:3D:4F:BE:66:F0:72:2F:72:43
    Signature Algorithm: ecdsa-with-SHA384
        30:64:02:30:5b:88:6e:08:bb:af:6b:58:18:62:8c:6c:34:a5:
        ec:b5:49:84:98:e5:ca:32:9c:d1:03:55:01:9d:0b:40:88:21:
        87:03:05:4d:ea:e4:bf:39:cf:5d:f1:07:aa:2a:08:fc:02:30:
        44:d1:b0:64:c5:56:48:8b:13:ea:33:d3:6d:1a:b0:6f:1c:39:
        0a:74:2f:b6:9c:e8:48:fd:46:bd:0a:07:74:e4:31:ef:2b:30:
        97:66:80:01:17:28:dd:e7:cb:e9:fc:cf
```

Table 1. STSAFE-TPM CA 0F certificate details

Field		Value
Version		3
Serial number		40h || F0h (that is, CA ID)
Signature algorithm		ecdsa-with-SHA384 (OID 1.2.840.10045.4.3.3)
Issuer		
	Country name	NL
	Organization name	STMicroelectronics nv
	Common name	STSAFE-TPM CA F0
Validity		
	Not before	20250206111717Z Generalized Time Value
	Not after	Never expires: 99991231235959Z Generalized Time Value
Subject		
	Country name	NL
	Organization name	STMicroelectronics nv
	Common name	STSAFE-TPM CA F0
Subject public key info		
	Algorithm	secp384r1 (OID 1.3.132.0.34)
	Subject public key	STSAFE-TPM CA F0 public key X, Y values
Extensions		
	Basic constraints	critical = TRUE
		cA=TRUE, pathLenConstraint = None
	Subject Key identifier	critical = FALSE
		keyIdentifier = SHA-1(04h || public key X || public key Y)
Signature algorithm		ecdsa-with-SHA384 (OID 1.2.840.10045.4.3.3)
Signature		R, S values of certificate signature (INTEGERS)

4 IAK / IDevID key-pair

The initial attestation key (IAK) and initial device ID (IDevID) are keys used for device attestation and authentication. The keys are set up within the ST33KTPM-IDevID so that the private key is never exposed.

The IAK is a “restricted” signing key, meaning it can only be used to sign data generated by the TPM. This is useful for *tpm2-quote* which signs a PCR value inside the TPM, enabling attestation capabilities.

The IDevID is a “non-restricted” signing key that can then be used to verify the device's authenticity. As a “non-restricted” signing key, it can be used to sign external data, allowing a device or cloud server to authenticate the TPM using the private key and associated IDevID certificate (as used in a TLS session with client authentication process).

5 IAK / IDevID leaf certificates

The IAK / IDevID leaf certificates are issued by the ST STSAFE-TPM CA.

Note: The TPM's RSA EK certificate is used for identifying information.

The X.509v3 subject alternative name (SAN) extension contains information to bind additional identity information to the subject of the leaf certificates.

5.1 Example of IAK certificate

```
Certificate:
    Data:
        Version: 3 (0x2)
        Serial Number:
41:cb:ba:61:28:f6:67:74)
        Signature Algorithm: ecdsa-with-SHA384
        Issuer: C=NL, O=STMicroelectronics nv, CN=STSAFE-TPM CA F0
        Validity
            Not Before: Sep  2 18:24:07 2025 GMT
            Not After : Dec 31 23:59:59 9999 GMT
        Subject: C=FR, O=STMicroelectronics, CN=ST1-TPM-CAF0-IA-CBBA6128F66774
        Subject Public Key Info:
            Public Key Algorithm: id-ecPublicKey
                Public-Key: (384 bit)
                pub:
                    04:d6:c3:a4:a0:c1:23:5a:e0:8a:ad:d8:a8:84:81:
                    4e:56:eb:86:ed:29:f0:e1:3b:21:83:e2:9e:a7:cf:
                    7e:37:b1:6d:47:2d:63:9f:41:02:62:c3:36:e2:45:
                    76:b4:5f:7a:f2:af:08:13:34:f2:4c:ee:c3:5f:b6:
                    e9:17:bd:e1:07:41:30:d3:d8:8b:55:46:b9:b6:e5:
                    8f:58:83:91:c2:cf:8a:db:a4:dd:c5:cf:12:02:e9:
                    d0:56:2a:fb:e8:3b:c4
                ASN1 OID: secp384r1
                NIST CURVE: P-384
        X509v3 extensions:
            X509v3 Key Usage:
                Digital Signature
            X509v3 Authority Key Identifier:
                62:86:0D:25:F2:60:20:6B:16:22:0A:3D:4F:BE:66:F0:72:2F:72:43
            X509v3 Subject Key Identifier:
                73:73:C7:47:A1:F5:BC:E0:F7:ED:9B:89:52:65:3F:EC:F7:2F:F5:20
            X509v3 Certificate Policies:
                Policy: 2.23.133.11.1.1
                Policy: 2.23.133.11.1.3
            X509v3 Basic Constraints:
                CA:FALSE
            X509v3 Subject Alternative Name:
                othername: 1.3.6.1.5.5.7.8.4::<unsupported>, othername: Permanent Identifier:
:<unsupported>
    Signature Algorithm: ecdsa-with-SHA384
    Signature Value:
        30:65:02:31:00:9e:91:89:1c:e4:f9:db:43:5f:38:b1:fb:71:
        c9:6e:6b:66:d9:4a:6f:64:3c:c2:dc:b0:d2:66:f6:3d:76:49:
        c8:f1:f6:90:69:ec:17:22:01:43:15:4c:71:bc:9f:a9:8f:02:
        30:5f:6b:59:9f:bf:39:f2:b3:c2:a5:e1:13:c8:2d:44:36:95:
        84:2a:d2:e0:76:5a:7c:d8:5f:a7:e9:0a:e0:9c:5a:f2:43:82:
        cb:c1:dd:e7:52:ce:58:14:3e:50:1c:8b:48
```

Table 2. IAK certificate template

Field		Value		
Version		3		
Serial number		41h || <(The ST33KTPM device's CPSN)>		
Signature algorithm		ecdsa-with-SHA384 (OID 1.2.840.10045.4.3.3)		
Issuer				
	Country name	NL		
	Organization name	STMicroelectronics nv		
	Common name	STSAFE-TPM CA F0		
Validity				
	Not before	<certificate creation date>		
	Not after	Never expires: 99991231235959Z Generalized Time Value		
Subject				
	Country name	FR		
	Organization name	STMicroelectronics		
	Common name	ST1-TPM-CAF0-IA-<(STSAFE-TPM's CPSN)>		
Subject public key info				
	Algorithm	secp384r1 (OID 1.3.132.0.34)		
	Subject public key	IAK public key X, Y values		
Extensions				
	Basic constraints	critical = FALSE (default)		
		cA=FALSE, pathLenConstraint = None		
	Key usage	critical = FALSE (default)		
		digitalSignature		
	Authority key identifier	critical = FALSE (default)		
		keyIdentifier = (CA Subject Key Identifier)		
	Subject key identifier	critical = FALSE (default)		
		keyIdentifier = SHA-1(04h || IAK public key X || IAK public key Y)		
	Certificate policies	critical = FALSE (default)		
		tcg-cap-verifiedTPMResidency (OID 2.23.133.11.1.1) tcg-cap-verifiedTPMRestricted (OID 2.23.133.11.1.3)		
	Subject alternative name (SAN)	critical = FALSE (default)		
		id-on-hardwareModuleName (OID 1.3.6.1.5.5.7.8.4)		
	-	-	hardwareModuleName (OID 2.23.133.1.2)	
			-	hwSerialNum = 'STM :' || <(EK authority key identifier)> || ':' || <(EK certificate serial number)> RSA 2048 EK Certificate (OCTET_STRING)
		id-on-permanentIdentifier (OID 1.3.6.1.5.5.7.8.3)		
		-	identifierValue = hexadecimal representation of SHA-256 digest of the RSA2048 EK Certificate (UTBF8String)	
			assigner = tcg-on-ekPermIdSha256 (OID 2.23.133.12.1)	
Signature algorithm		ecdsa-with-SHA384 (OID 1.2.840.10045.4.3.3)		
Signature		R, S values of certificate signature (INTEGERS)		

5.2 Example of IDevID

```
Certificate:
    Data:
        Version: 3 (0x2)
        Serial Number:
42:cb:ba:61:28:f6:67:74)
        Signature Algorithm: ecdsa-with-SHA384
        Issuer: C=NL, O=STMicroelectronics nv, CN=STSAFE-TPM CA F0
        Validity
            Not Before: Sep  2 18:24:18 2025 GMT
            Not After : Dec 31 23:59:59 9999 GMT
        Subject: C=FR, O=STMicroelectronics, CN=ST1-TPM-CAF0-ID-CBBA6128F66774
        Subject Public Key Info:
            Public Key Algorithm: id-ecPublicKey
                Public-Key: (384 bit)
                pub:
                    04:f7:b3:b3:e0:ad:83:df:f9:93:7f:52:43:17:c2:
                    bc:40:c6:20:0f:7e:05:2b:f0:cc:46:e6:9e:c4:ed:
                    a6:e6:d3:70:77:3d:49:04:50:69:46:1a:19:f9:01:
                    c3:c9:04:64:0d:42:23:5e:ab:60:97:37:c4:06:a5:
                    33:6e:1f:b7:cd:51:72:db:ff:7c:52:15:8a:01:e7:
                    2d:4f:d8:35:42:db:3a:6f:e0:c7:c7:8a:91:12:8f:
                    80:bb:b0:4b:0c:85:d9
                ASN1 OID: secp384r1
                NIST CURVE: P-384
        X509v3 extensions:
            X509v3 Key Usage:
                Digital Signature
            X509v3 Authority Key Identifier:
                62:86:0D:25:F2:60:20:6B:16:22:0A:3D:4F:BE:66:F0:72:2F:72:43
            X509v3 Subject Key Identifier:
                8B:4E:BE:32:F9:66:68:8D:16:E0:18:67:86:B0:88:96:9C:A3:10:BB
            X509v3 Certificate Policies:
                Policy: 2.23.133.11.1.1
                Policy: 2.23.133.11.1.2
                Policy: 2.23.133.11.1.4
            X509v3 Basic Constraints:
                CA:FALSE
            X509v3 Subject Alternative Name:
                othername: 1.3.6.1.5.5.7.8.4::<unsupported>, othername: Permanent Identifier:
:<unsupported>
    Signature Algorithm: ecdsa-with-SHA384
    Signature Value:
        30:65:02:30:37:87:41:6e:66:8f:f5:a1:39:12:0e:04:8d:85:
        0a:d0:6e:05:c3:6d:a6:2d:bc:05:2d:f7:5b:f7:bb:59:de:87:
        91:6b:e3:3c:e4:22:f8:fe:29:85:9e:40:c0:68:76:07:02:31:
        00:ff:01:9d:2d:7a:a0:7d:8e:1d:f4:ba:7b:16:b7:73:53:ba:
        75:0a:39:14:54:ee:ee:50:0e:e5:c4:9e:bd:6c:57:1d:e1:91:
        05:e3:5b:92:55:1c:e5:78:19:86:64:88:0b
```

Table 3. IDevID certificate template

Field		Value		
Version		3		
Serial number		42h || <(TPM's CPSN)>		
Signature algorithm		ecdsa-with-SHA384 (OID 1.2.840.10045.4.3.3)		
Issuer				
	Country name	NL		
	Organization name	STMicroelectronics nv		
	Common name	STSAFE-TPM CA F0		
Validity				
	Not before	<certificate creation date>		
	Not after	Never expires: 99991231235959Z Generalized Time Value		
Subject				
	Country name	FR		
	Organization name	STMicroelectronics		
	Common name	ST1-TPM-CAF0-ID-<(TPM's CPSN)>		
Subject public key info				
	Algorithm	secp384r1 (OID 1.3.132.0.34)		
	Subject public key	IDevID public key X, Y values		
Extensions				
	Basic constraints	critical = FALSE (default)		
		cA=FALSE, pathLenConstraint = None		
	Key usage	critical = FALSE (default)		
		digitalSignature		
	Authority key identifier	critical = FALSE (default)		
		keyIdentifier = *(CA Subject Key Identifier)*		
	Subject key identifier	critical = FALSE (default)		
		keyIdentifier = SHA-1(04h || IDevID public key X || IDevID public key Y)		
	Certificate policies	critical = FALSE (default)		
		tcg-cap-verifiedTPMResidency (OID 2.23.133.11.1.1) tcg-cap-verifiedTPMFixed (OID 2.23.133.11.1.2) tcg-cap-intendedUseDevID (2.23.133.11.1.4)		
	Subject alternative name (SAN)	critical = FALSE (default)		
	-	id-on-hardwareModuleName (OID 1.3.6.1.5.5.7.8.4)		
		-	hardwareModuleName (OID 2.23.133.1.2)	
			-	hwSerialNum = 'STM :' || <(EK Authority Key identifier)> || ':' || RSA 2048 EK <(EK Certificate serial number)> RSA 2048 EK (OCTET_STRING)
		id-on-permanentIdentifier (OID 1.3.6.1.5.5.7.8.3)		
		-	identifierValue = hexadecimal representation of SHA-256 digest of the RSA 2048 EK Certificate (UTF8String)	
			assigner = tcg-on-ekPermIdSha256 (OID 2.23.133.12.1)	
Signature algorithm		ecdsa-with-SHA384 (OID 1.2.840.10045.4.3.3)		
Signature		R, S values of certificate signature (INTEGERS)		

6 Master authorization values

Each master authentication value is different, and the customer is responsible for the protection of the derived authorization values in their final products.

Master key for IDevID and IAK keys `authvalue` derivation =

```
{0x6B,0x83,0x29,0x9A,0xB3,0x5E,0x28,0xEE,
0xB3,0x0A,0x63,0xF7,0xA6,0xA0,0xA7,0xAE};
```

Master key for owner hierarchy authvalue derivation =

```
{Unknown Random Value};
```

Master key for endorsement hierarchy `authvalue` derivation =

```
{0xA4,0x02,0x41,0x76,0xE0,0x47,0xF4,0xA5,
0x77,0x4D,0x2C,0x02,0xDD,0x16,0x9B,0xCA};
```

Master key for lockout hierarchy `authvalue` derivation =

```
{0x7E,0x5D,0x09,0x86,0x0F,0x93,0x72,0x9F,
0x2B,0xD7,0x1D,0xC5,0xBB,0xEA,0xF8,0xF0};
```

7 Using the IAK / IDevID keys

To wield the IAK and IDevID private keys inside of the ST33KTPM-IDevID, an `authValue` (or password) must be used.

Note: An `authValue` is not required to read the leaf certificates.

The key `authValue` is derived from the SHA-256 of the ST33KTPM device unique serial number (CPSN) and a master key authorization value.

Example: `authValue` = lower 128-bits of the result from the SHA-256 (serial number || Master_Key authorization value)

7.1 Example of IAK / IDevID usage

Given,

```
CPSN = 0B:3A:80:01:EE:7B:88
Master Key Authentication Value = 6B:83:29:9A:B3:5E:28:EE:B3:0A:63:F7:A6:A0:A7:AE
```

Compute,

```
SHA256(0B:3A:80:01:EE:7B:88:6B:83:29:9A:B3:5E:28:EE:B3:
0A:63:F7:A6:A0:A7:AE ) = 49:D9:80:E2:46:42:43:04:01:A7:0B:AC:17:6F:4C:35
84:80:42:3F:F6:4D:DD:52:60:11:DC:52:28:1A:63:E3
```

Hence, the derived `authValue` =

```
84:80:42:3F:F6:4D:DD:52:60:11:DC:52:28:1A:63:E3
```

8 Storage of IAK / IDevID keys and certificates

In the ST33KTPM-IDevID devices, the IAK and IDevID keys cannot be deleted (evicted) using the `TPM2_EvictControl` command with the platform or owner hierarchy authorization. IAK and IDevID keys have the dictionary attack mitigation feature enabled, and the lockout hierarchy authorization value is used to reset the dictionary attack failures or to exit from dictionary attack lockout if reached. The endorsement hierarchy authorization value enables the creation of AK and DevID keys, with the appropriate template (refer to Section 8.1: Primary key create template) allowing the creation of LDevID and LAK keys.

STMicroelectronics provides the master authorization values for the endorsement and lockout hierarchies. The device-specific authorization values are derived in the same manner as the key `AuthValue`, using the appropriate master authorization value for the hierarchy.

ST33KTPM-IDevID devices are shipped with the `TPM_Clear` command disabled and permanently locked.

Note: This behavior deviates from the TPM library specification and is meant to thwart any denial-of-service attack if the IDevID and IAK certificates are deleted from TPM memory.

8.1 Primary key create template

This template is used with `TPM2_CreatePrimary` to create the LAK and LDevID.

Template:

- disableClear = Set
- ehEnabled = Set
- endorsementAlg = HMAC
- endorsementPolicy = empty

objectAttributes :

- fixedTPM = 1
- stClear = 0
- fixedParent = 1
- sensitiveDataOrigin = 1
- userWithAuth = 1
- adminWithPolicy = 0*
- noDA = 0
- encryptedDuplication = 0
- DevID (signing): Restricted = 0 or AK (signing): Restricted = 1
- decrypt = 0
- sign = 1
- authValue = password

ECC NIST P-384 parameters:

- type = TPM_ALG_ECC
- nameAlg = TPM_ALG_SHA384
- objectAttributes (as above)
- authPolicy = TPM2B_DIGEST
- size = 0*
- parameters = TPMS_ECC_PARMS
- symmetric->algorithm = TPM_ALG_NULL
- symmetric->keyBits = NULL
- symmetric->mode = NULL
- symmetric->details = NULL
- scheme->scheme = TPM_ALG_ECDSA
- scheme->details = TPM_ALG_SHA384*
- curveID = TPM_ECC_NIST_P384
- kdf->scheme = TPM_ALG_NULL

- kdf->details = NULL
- unique
- x->size
- x->buffer = ‘IDEVID’ (0x49,0x44,0x45,0x56,0x49,0x44) or ‘IAK’ (0x49,0x41,0x4B)
- y->size
- y->buffer

Note: This symbol (*) indicates the necessary differences from the TCG specification.

Note: ECDSA is limited to signing SHA384 digests.

9 TPM handles

Table 4. **TPM handles**

-	IAK	DevID
Key handle	0x81020001	0x81020000
Certificate NVM handle	0x01C90100	0x01C90200

10 Bundle files

To facilitate registration of leaf certificates, a bundle file is provided for each reel of provisioned ST33KTPM-IDevID devices.

Each reel is provided with a unique identifier used to identify the certificate bundle file in a database.

The bundle file contains a manifest of all the IAK and the IDevID certificates for all the devices in the reel.

The bundle file is a ZIP file that contains:

- One manifest ledger XML file that holds the diversifier information and the leaf certificates for every ST33KTPM-IDevID in the reel
- One pair of leaf certificates (IAK and IDevID) per ST33KTPM-IDevID device

Manifest ledger XML file

The reel manifest XML file structure is defined as below:

```
<root>
    <PERSO_DATA>
        <DIVERSIFICATION_DATA>(diversifier TPM chip 1)</DIVERSIFICATION_DATA>
        <IAK_CERTIFICATE_SIGNED_BY_CA_DATA>
            (IAK leaf certificate for TPM chip 1)
        </IAK_CERTIFICATE_SIGNED_BY_CA_DATA>
        <IDEVID_CERTIFICATE_SIGNED_BY_CA_DATA>
            (IDevID leaf certificate for TPM chip 1)
        </IDEVID_CERTIFICATE_SIGNED_BY_CA_DATA>
    </PERSO_DATA>
    . . .
    . . .
    <PERSO_DATA>
        <DIVERSIFICATION_DATA>(diversifier TPM chip n)</DIVERSIFICATION_DATA>
        <IAK_CERTIFICATE_SIGNED_BY_CA_DATA>
            (IAK leaf certificate for TPM chip n)
        </IAK_CERTIFICATE_SIGNED_BY_CA_DATA>
        <IDEVID_CERTIFICATE_SIGNED_BY_CA_DATA>
            (IDevID leaf certificate for TPM chip n)
        </IDEVID_CERTIFICATE_SIGNED_BY_CA_DATA>
    </PERSO_DATA>
</root>
```

Note: The different fields included in the manifest ledger XML file are described in Table 5.

Table 5. XML file and fields description

Field	Description
`Diversifier TPM chip <i>`	Unique serial number (CPSN) of the TPM chip <i> in hexadecimal format (14 digits).
`IAK leaf certificate for TPM chip <i>`	Computed IAK certificate for a ST33KTPM-IDevID device, in PEM format, base64 encoded.
`IDevID leaf certificate for TPM chip <i>`	Computed IDevID certificate for a ST33KTPM-IDevID device, in PEM format, base64 encoded.

10.1 Leaf certificate file format

For each provisioned TPM chip, the IAK and IDevID certificates are stored as individual files. These certificates are stored as text files in PEM format, base64 encoded.

The certificate files are named after the hexadecimal CPSN value of the TPM chip:

- <CPSN>_IAK.cer
- <CPSN>_IDevID.cer

For example, for each ST33KTPM (with serial number (CPSN) = `5B44E0C9E76A98`):

- `5B44E0C9E76A98_IAK.cer`
- `5B44E0C9E76A98_IDevID.cer`

11 Customer-specific provisioning profile

STMicroelectronics offers the ability to customize the ST33KTPM-IDevID with a customer-specific profile limited to the features described in the following sections.

This customization allows customers to use automated cloud enrollment schemes such as AWS IoT Just-In-Time Registration (JITR/JITP) service and Microsoft Azure Device Provisioning Service (DPS).

For further information, contact your local sales representative.

11.1 Customization options

STMicroelectronics assigns a unique STSAFE-TPM CA for each customer and is also able to provide CA validation certificates for cloud service enrollment. Refer to Section 11.3: STSAFE-TPM CA validation service for more information.

The customer can customize the following two fields in the leaf certificates, as shown below:

- Subject::Common Name header which is concatenated with the assigned CA label (xx) and TPM serial number (for example, <CN_Header>-TPM-CA<xx>-ID-<CPSN>).
- Subject::Organization Name

Note: The customer is responsible to ensure that the name complies with cloud service standards. Refer to Section 11.4: Common name for more information. If left unassigned, the ST default value "VC" is used. Also, if the customer specifies <CN_Header> , it must comply with cloud service standards, if applicable.

For each profile, STMicroelectronics generates the master authentication values using a random number generator. The access control authentication values can be customized as follows:

- Master key authentication value: assigned by STMicroelectronics.
- – Key `AuthValue` is derived using the master key `AuthValue` and the ST33KTPM-IDevID unique serial number (CPSN).
- Master owner hierarchy authentication value: assigned by STMicroelectronics.
  - OH `AuthValue` is derived using the master OH `AuthValue` and the ST33KTPM-IDevID unique serial number (CPSN).
- Master endorsement hierarchy authentication value : assigned by STMicroelectronics.
  - EH `AuthValue` is derived using the master EH `AuthValue` and the ST33KTPM-IDevID unique serial number (CPSN).
- Master lockout authentication value: assigned by STMicroelectronics.
  - LO `AuthValue` is derived using the master LO `AuthValue` and the ST33KTPM-IDevID unique serial number (CPSN).
- The `TPM_Clear` command permanent disable option.

Table 6. Customer specific profile form

-	Type	STMicroelectronics default values	Customer request	Notes
CA	Byte value	-	To be assigned	STMicroelectronics to share CA certificate
Common name header (CN_Header)	Up to 16 characters	“VC”	""	String of printable characters
Organization name	Up to 32 characters	“STMicroelectronics”	""	String of printable characters
-				
Master key auth. value	16 bytes	-	-	Generated by STMicroelectronics
Share	Yes	Yes	Yes	STMicroelectronics to share
-				
Master OH auth. value	16 bytes	-	-	Generated by STMicroelectronics
Share	Yes/No	No	Yes/No	Permission to share
-				
Master EH auth. value	16 bytes	-	-	Generated by STMicroelectronics
Share	Yes/No	Yes	Yes/No	Permission to share
-				
Master LO auth. value	16 bytes	-	-	Generated by STMicroelectronics
Share	Yes	Yes	Yes	STMicroelectronics to share
-				
TPM Clear Permanent Disable	Yes/No	Yes	Yes/No	-

Note: Shared master authorization values are provided over a secure communication channel using PGP encryption.

11.2 ST STSAFE-TPM CA

STMicroelectronics assigns an STSAFE-TPM CA to a customer, and the CA certificate includes the following:

- Issuer/Subject common name (for example, STSAFE-TPM CA xx)
- Validity not before value is set to the date it was issued
- Validity not after value is set to never expire (99991231235959Z)
- Unique EC key-pair

11.3 STSAFE-TPM CA validation service

Customers wishing to enroll their assigned STSAFE-TPM CA with either Azure or AWS IoT cloud service must provide their verification code to STMicroelectronics. In return, STMicroelectronics provides a corresponding verification certificate, signed by their assigned STSAFE-TPM CA.

11.4 Common name

The certificates Subject::Common Name needs to comply with TCG specification 802.1AR requirement as well as the naming conventions used by Microsoft Azure and AWS IoT.

The certificate Subject::Common Name field for the x.509 device has to be a unique text string (of permitted characters) without spaces.

1. AWS IoT (permitted characters): **`[a-zA-Z0-9:_-]+`**
2. Microsoft Azure (permitted characters): **`(a-zA-Z0-9:_-)+.,%#*?!:=@$'`**
3. Appending the STSAFE-TPM serial number to a text string ensures uniqueness.

The Subject::Common Name field format appears as follows:

```
<CN_Header>-TPM-CAxx-<Type>-<device serial number>
```

- Where CN header (common name header) is a text string provided by the customer, or set to “VC” if none is provided. The text should comply with naming conventions mentioned above, and is limited to 32 readable characters
- Where xx is the CA key identifier
- Where type is “IA” for IAK and “ID” for IDevID

Note: Subject::Common Name examples:

- *VC-TPM-CAxx-IA-5B44E0C9E76A98*
- *VC-TPM-CAxx-ID-5B44E0C9E76A98*

12 Examples (Linux TPM2 tools and OpenSSL)

12.1 IAK

The user must read the TPM serial number into the *SN_raw.txt* file, and put the master password into binary file.

```
cat SN_raw.txt masterPwd.bin > password.bin

tpm2_hash -g sha256 -o hashPwd.bin password.bin

split -b16 hashPwd.bin finalPwd # Splits into finalPwdaa and finalPwdab

PASSWORD=$(xxd -p -c 100 finalPwdab | tr -d '\n')

tpm2_quote -Q -c 0x81020001 -l sha384:0 -f plain -m Test.dat -s sig.ecc -p hex:$PASSWORD

tpm2 nvread 0x1C90100 > IAK_Certificate.der

openssl verify -CAfile CA_rootCA.pem IAK_Certificate.der

openssl x509 -in IAK_Certificate.der -inform DER -pubkey -noout > IAK_PubKey.pem

openssl dgst -sha384 -verify IAK_PubKey.pem -keyform pem -signature sig.ecc  Test.dat
```

Password calculated/present if `authvalue` is set.

12.2 IDevID

In this example, the user must assume that the password has been calculated previously (refer to Section 12.1: IAK).

```
PASSWORD=$(xxd -p -c 100 finalPwdab | tr -d '\n')

tpm2_sign -Q -c 0x81020000 -g sha384 -o sig.ecc message.dat -p hex:$PASSWORD

tpm2 nvread 0x1C90200 > IDevID_Certificate.der

openssl x509 -in IDevID_Certificate.der -inform DER -pubkey -noout

openssl verify -CAfile CA_rootCA.pem IDevID_Certificate.der

openssl x509 -in IDevID_Certificate.der -inform DER -pubkey -noout > IDevID_PubKey.pem

openssl dgst -sha384 -verify IDevID_PubKey.pem -keyform pem -signature sig.ecc message.dat
```

Password calculated/present if `authvalue` is set.

Appendix A Reference documents

Table 7. Reference documents

Reference	Document details
[TPM 2.0 IDevID &IAK 1.1]	*TPM 2.0 Keys for Device Identity and Attestation*, Version 1.1, April 23, 2025, Trusted Computing Group.
[TCG EK Cre Profile TPM 2.3]	*TCG EK credential profile for TPM Family 2.0 Level 0. Specification*, Version 2.3 Revision 2, 23 July 2020, TCG.
[DS15011]	*ST33KTPM provisioned with keys for device identity and attestation*, ST33KTPM-IDevID datasheet, revision 1, STMicroelectronics.

Revision history

Table 8. **Document revision history**

Date	Revision	Changes
20-Oct-2025	1	Initial release.

Contents

List of tables

List of figures

IMPORTANT NOTICE – READ CAREFULLY

STMicroelectronics NV and its subsidiaries (“ST”) reserve the right to make changes, corrections, enhancements, modifications, and improvements to ST products and/or to this document at any time without notice.

In the event of any conflict between the provisions of this document and the provisions of any contractual arrangement in force between the purchasers and ST, the provisions of such contractual arrangement shall prevail.

The purchasers should obtain the latest relevant information on ST products before placing orders. ST products are sold pursuant to ST’s terms and conditions of sale in place at the time of order acknowledgment.

The purchasers are solely responsible for the choice, selection, and use of ST products and ST assumes no liability for application assistance or the design of the purchasers’ products.

No license, express or implied, to any intellectual property right is granted by ST herein.

Resale of ST products with provisions different from the information set forth herein shall void any warranty granted by ST for such product.

If the purchasers identify an ST product that meets their functional and performance requirements but that is not designated for the purchasers' market segment, the purchasers shall contact ST for more information.

ST and the ST logo are trademarks of ST. For additional information about ST trademarks, refer to www.st.com/trademarks. All other product or service names are the property of their respective owners.

Information in this document supersedes and replaces information previously supplied in any prior versions of this document.