TN1330

Technical note

ST Trusted Platform Module (TPM) endorsement key (EK) certificates

Introduction

This document presents the STMicroelectronics trusted platform module (TPM) endorsement key (EK) certificates.

Primarily, these TPM certificates provide an evidence, endorsed by an independent certification authority (CA), that the TPM used is genuine.

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

Root certificates are signed by the independent Globalsign® CA for most products.

Dedicated intermediate certificates can also be issued to differentiate various ST TPM product technologies or final applications.

This technical note applies to the products listed in the following table.

Table 1. **List of products**

Type	Products
Secure microcontroller	ST33TPM12LPC ST33TPM12I2C ST33TPM12SPI
	ST33TPHF2ESPI ST33TPHF20SPI ST33TPHF2EI2C ST33TPHF20I2C ST33TPHF2XSPI ST33TPHF2XSPI-C1 ST33TPHF2XI2C ST33TPHF2XI2C-C1
	ST33GTPMASPI ST33GTPMAI2C ST33GTPMISPI ST33GTPMII2C
	ST33KTPM2XSPI ST33KTPM2XI2C ST33KTPM2X
	ST33KTPM2I STSAFE-V100-TPM

This document provides downloadable links to ST TPM EK certificate files.

1 TPM EK certificate

STMicroelectronics embeds a TPM EK certificate in all its TPM products during the TPM manufacturing phase.

STMicroelectronics operates its own certificate authority, which is root-certified by the independent GlobalSign certification authority for most of the products. Several intermediate certificate authorities can be created in order to discriminate different major application revisions or product technologies. The following tables define the current links between intermediate CAs and product sales types.

Table 2. **RSA intermediate CAs (for RSA 2048-bit EKs) and TPM products (at the time of publication)**

CA common name	Products	Commercial part number	Firmware revision
ST Intermediate CA 02	ST33TPM12LPC	ST33ZP24PVSC	13.00
	ST33TPM12LPC	ST33ZP24PVSH	13.08
	ST33TPM12I2C	ST33ZP24PVSK	13.10
	ST33TPM12SPI	ST33ZP24PVSL	13.11
	ST33TPM12LPC	ST33ZP24PVSP	13.12
ST Intermediate CA 03	ST33TPM12LPC	ST33ZP24PVSM	13.08
ST Intermediate CA 04	ST33TPMF2ESPI	ST33HTPMAAD8	70.00
	ST33TPMF2ESPI	ST33HTPMAAE0	70.00
ST Intermediate CA 05	ST33TPHF2ESPI	ST33HTPHAAE5	71.00
	ST33TPHF2ESPI	ST33HTPHAAE6	71.00
	ST33TPHF20SPI	ST33HTPHAAE8	72.00
	ST33TPHF2ESPI	ST33HTPHAHA5	71.04
	ST33TPHF2ESPI	ST33HTPHAHA6	71.04
	ST33TPHF2ESPI	ST33HTPHAAF0	73.00
	ST33TPHF2ESPI	ST33HTPHAAF1	73.00
	ST33TPHF20SPI	ST33HTPHAAF3	74.00
	ST33TPHF2ESPI	ST33HTPHAHB3	73.04
	ST33TPHF2ESPI	ST33HTPHAHB4	73.04
	ST33TPHF2EI2C	ST33HTPHAHB7	73.05
	ST33TPHF2EI2C	ST33HTPHAHB8	73.05
	ST33TPHF20I2C	ST33HTPHAHB9	74.05
	ST33TPHF2ESPI	ST33HTPHAHC0	73.08
	ST33TPHF20SPI	ST33HTPHAHC1	74.08
	ST33TPHF2EI2C	ST33HTPHAHC2	73.09
	ST33TPHF20I2C	ST33HTPHAHC3	74.09
	ST33TPHF20SPI	ST33HTPHAHC9	74.16
	ST33TPHF2ESPI	ST33HTPHAHD6	73.20
	ST33TPHF20SPI	ST33HTPHAHD7	74.20
	ST33TPHF2ESPI	ST33HTPHAHD0	73.64
	ST33TPHF20SPI	ST33HTPHAHD1	74.64

CA common name	Products	Commercial part number	Firmware revision
ST Intermediate CA 06	ST33TPHF2XSPI	ST33HTPHAHC4	1.256
	ST33TPHF2XSPI	ST33HTPHAHD4	1.257
	ST33TPHF2XSPI	ST33HTPHAHD8	1.258
	ST33TPHF2XSPI	ST33HTPHAHE0	1.512
	ST33TPHF2XSPI-C1	ST33HF2X32AHE2C1	1.512
	ST33TPHF2XSPI	ST33HTPHAHE4	1.769
	ST33TPHF2XI2C	ST33HTPHAHC5	2.256
	ST33TPHF2XI2C	ST33HTPHAHD5	2.272
	ST33TPHF2XI2C	ST33HTPHAHE1	2.512
	ST33TPHF2XI2C-C1	ST33HF2X32AHE2C1	2.512
ST Intermediate CA 07	ST33GTPMASPI	ST33GTPMA020FAE5	3.256
	ST33GTPMAI2C	ST33GTPMA020FAE6	6.256
	ST33GTPMISPI	ST33GTPMIWLFZE4	3.257
	ST33GTPMII2C	ST33GTPMIWLFZE5	6.257
STSAFE TPM RSA Intermediate CA 10	ST33KTPM2XSPI	ST33KTPM2XxxCKE2	9.256
	ST33KTPM2XI2C	ST33KTPM2XxxCKE3	9.256
	ST33KTPM2XSPI	ST33KTPM2XxxDKG8	9.257
	ST33KTPM2X	ST33KTPM2XxxDKG9	9.257
	ST33KTPM2XSPI	ST33KTPM2XxxDKJ5	9.258
	ST33KTPM2XSPI	ST33KTPM2XxxDKJ0	9.512
	ST33KTPM2X	ST33KTPM2XxxDKJ1	9.512
STSAFE TPM RSA Intermediate CA 20	STSAFE-V100-TPM	ST33KTPM2AxxBAC5	10.257
	ST33KTPM2I	ST33KTPM2IxxBZA9	10.257
	STSAFE-V100-TPM	STSAFV10TMxxBAD6	10.512
	ST33KTPM2I	ST33KTPM2IxxBZB1	10.512

Table 3. **RSA Intermediate CAs (for RSA 3072-bit EKs) and TPM products (at the time of publication)**

CA common name	Products	Commercial part number	Firmware revision
STSAFE TPM RSA Intermediate CA 11	ST33KTPM2XSPI	ST33KTPM2XxxDKJ5	9.258
	ST33KTPM2XSPI	ST33KTPM2XxxDKJ0	9.512
	ST33KTPM2X	ST33KTPM2XxxDKJ1	9.512
STSAFE TPM RSA Intermediate CA 21	STSAFE-V100-TPM	STSAFV10TMxxBAD6	10.512
	ST33KTPM2I	ST33KTPM2IxxBZB1	10.512

Table 4. **ECC intermediate CAs (for ECC_256 EKs) and TPM products (at the time of publication)**

CA common name	Products	Commercial part numbers	Firmware revision
STM TPM ECC Intermediate CA 01	ST33TPHF2ESPI	ST33HTPHAAE5	71.00
	ST33TPHF2ESPI	ST33HTPHAAE6	71.00
	ST33TPHF20SPI	ST33HTPHAAE8	72.00
	ST33TPHF2ESPI	ST33HTPHAHA5	71.04
	ST33TPHF2ESPI	ST33HTPHAHA6	71.04
	ST33TPHF2ESPI	ST33HTPHAAF0	73.00
	ST33TPHF2ESPI	ST33HTPHAAF1	73.00
	ST33TPHF2ESPI	ST33HTPHAHB3	73.04
	ST33TPHF2ESPI	ST33HTPHAHB4	73.04
	ST33TPHF20SPI	ST33HTPHAAF3	74.00
	ST33TPHF2EI2C	ST33HTPHAHB7	73.05
	ST33TPHF2EI2C	ST33HTPHAHB8	73.05
	ST33TPHF20I2C	ST33HTPHAHB9	74.05
	ST33TPHF2ESPI	ST33HTPHAHC0	73.08
	ST33TPHF20SPI	ST33HTPHAHC1	74.08
	ST33TPHF2EI2C	ST33HTPHAHC2	73.09
	ST33TPHF20I2C	ST33HTPHAHC3	74.09
	ST33TPHF20SPI	ST33HTPHAHC9	74.16
	ST33TPHF2ESPI	ST33HTPHAHD6	73.20
	ST33TPHF20SPI	ST33HTPHAHD7	74.20
	ST33TPHF2ESPI	ST33HTPHAHD0	73.64
	ST33TPHF20SPI	ST33HTPHAHD1	74.64
STM TPM ECC Intermediate CA 02	ST33TPHF2XSPI	ST33HTPHAHC4	1.256
	ST33TPHF2XSPI	ST33HTPHAHD4	1.257
	ST33TPHF2XSPI	ST33HTPHAHD8	1.258
	ST33TPHF2XSPI	ST33HTPHAHE0	1.512
	ST33TPHF2XSPI	ST33HTPHAHE4	1.769
	ST33TPHF2XI2C	ST33HTPHAHC5	2.256
	ST33TPHF2XI2C	ST33HTPHAHD5	2.272
	ST33TPHF2XI2C	ST33HTPHAHE1	2.512
STM TPM ECC Intermediate CA 03	ST33GTPMASPI	ST33GTPMA020FAE5	3.256
	ST33GTPMAI2C	ST33GTPMA020FAE6	6.256
	ST33GTPMISPI	ST33GTPMIWLFZE4	3.257
	ST33GTPMII2C	ST33GTPMIWLFZE5	6.257
STSAFE TPM ECC Intermediate CA 10	ST33KTPM2XSPI	ST33KTPM2XxxCKE2	9.256
	ST33KTPM2XI2C	ST33KTPM2XxxCKE3	9.256
	ST33KTPM2XSPI	ST33KTPM2XxxDKG8	9.257
	ST33KTPM2X	ST33KTPM2XxxDKG9	9.257
	ST33KTPM2XSPI	ST33KTPM2XxxDKJ5	9.258
	ST33KTPM2XSPI	ST33KTPM2XxxDKJ0	9.512
	ST33KTPM2X	ST33KTPM2XxxDKJ1	9.512

CA common name	Products	Commercial part numbers	Firmware revision
STSAFE TPM ECC Intermediate CA 20	STSAFE-V100-TPM	ST33KTPM2AxxBAC5	10.257
	ST33KTPM2I	ST33KTPM2IxxBZA9	10.257
	STSAFE-V100-TPM	STSAFV10TMxxBAD6	10.512
	ST33KTPM2I	ST33KTPM2IxxBZB1	10.512

Table 5. ECC intermediate CAs (for ECC 384 EKs) and TPM products

CA common name	Products	Commercial part numbers	Firmware revision
STM TPM ECC384 Intermediate CA 01	ST33TPHF2XSPI	ST33HTPHAHC4	1.256
	ST33TPHF2XSPI	ST33HTPHAHD4	1.257
	ST33TPHF2XSPI	ST33HTPHAHD8	1.258
	ST33TPHF2XSPI	ST33HTPHAHE0	1.512
	ST33TPHF2XSPI	ST33HTPHAHE4	1.769
	ST33TPHF2XI2C	ST33HTPHAHC5	2.256
	ST33TPHF2XI2C	ST33HTPHAHD5	2.272
	ST33TPHF2XI2C	ST33HTPHAHE1	2.512
STM TPM ECC384 Intermediate CA 02	ST33GTPMASPI	ST33GTPMA020FAE5	3.256
	ST33GTPMAI2C	ST33GTPMA020FAE6	6.256
	ST33GTPMISPI	ST33GTPMIWLFZE4	3.257
	ST33GTPMII2C	ST33GTPMIWLFZE5	6.257
STM TPM ECC384 Intermediate CA 03 for CISCO	ST33TPHF2XSPI-C1	ST33HF2X32AHE2C1	1.512
	ST33TPHF2XI2C-C1	ST33HF2X32AHE3C1	2.512
STSAFE TPM ECC Intermediate CA 11	ST33KTPM2XSPI	ST33KTPM2XxxCKE2	9.256
	ST33KTPM2XI2C	ST33KTPM2XxxCKE3	9.256
	ST33KTPM2XSPI	ST33KTPM2XxxDKG8	9.257
	ST33KTPM2X	ST33KTPM2XxxDKG9	9.257
	ST33KTPM2XSPI	ST33KTPM2XxxDKJ5	9.258
	ST33KTPM2XSPI	ST33KTPM2XxxDKJ0	9.512
	ST33KTPM2X	ST33KTPM2XxxDKJ1	9.512
STSAFE TPM ECC Intermediate CA 21	STSAFE-V100-TPM	ST33KTPM2AxxBAC5	10.257
	ST33KTPM2I	ST33KTPM2IxxBZA9	10.257
	STSAFE-V100-TPM	STSAFV10TMxxBAD6	10.512
	ST33KTPM2I	ST33KTPM2IxxBZB1	10.512

Table 6. RSA TPM CA certificate URLs

Certificate common name	File/Link
GlobalSign Trusted Computing CA	https://secure.globalsign.com/cacert/gstpmroot.crt or http://secure.globalsign.com/cacert/gstpmroot.crt
ST TPM Root certificate	https://secure.globalsign.com/cacert/stmtpmekroot.crt or http://secure.globalsign.com/cacert/stmtpmekroot.crt
STSAFE RSA Root CA 02	http://sw-center.st.com/STSAFE/STSAFERsaRootCA02.crt or https://sw-center.st.com/STSAFE/STSAFERsaRootCA02.crt
ST Intermediate CA 01	https://secure.globalsign.com/cacert/stmtpmekint01.crt or http://secure.globalsign.com/cacert/stmtpmekint01.crt

Certificate common name	File/Link
ST Intermediate CA 02	https://secure.globalsign.com/cacert/stmtpmekint02.crt or http://secure.globalsign.com/cacert/stmtpmekint02.crt
ST Intermediate CA 03	https://secure.globalsign.com/cacert/stmtpmekint03.crt or http://secure.globalsign.com/cacert/stmtpmekint03.crt
ST Intermediate CA 04	https://secure.globalsign.com/cacert/stmtpmekint04.crt or http://secure.globalsign.com/cacert/stmtpmekint04.crt
ST Intermediate CA 05	https://secure.globalsign.com/cacert/stmtpmekint05.crt or http://secure.globalsign.com/stmtpmekint05.crt
ST Intermediate CA 06	https://secure.globalsign.com/cacert/stmtpmekint06.crt or http://secure.globalsign.com/stmtpmekint06.crt
ST Intermediate CA 07	https://secure.globalsign.com/cacert/stmtpmekint07.crt or http://secure.globalsign.com/stmtpmekint07.crt
STSAFE TPM RSA Intermediate CA 10	http://sw-center.st.com/STSAFE/stsafetpmrsaint10.crt or https://sw-center.st.com/STSAFE/stsafetpmrsaint10.crt
STSAFE TPM RSA Intermediate CA 11	http://sw-center.st.com/STSAFE/stsafetpmrsaint11.crt or https://sw-center.st.com/STSAFE/stsafetpmrsaint11.crt
STSAFE TPM RSA Intermediate CA 20	http://sw-center.st.com/STSAFE/stsafetpmrsaint20.crt or https://sw-center.st.com/STSAFE/stsafetpmrsaint20.crt
STSAFE TPM RSA Intermediate CA 21	http://sw-center.st.com/STSAFE/stsafetpmrsaint21.crt or https://sw-center.st.com/STSAFE/stsafetpmrsaint21.crt

Table 7. **ECC TPM CA certificate URLs**

Certificate common name	File/Link
GlobalSign Trusted Platform Module ECC Root CA	https://secure.globalsign.com/cacert/tpmeccroot.crt or http://secure.globalsign.com/cacert/tpmeccroot.crt
STM TPM ECC Root CA 01	https://secure.globalsign.com/cacert/stmtpmeccroot01.crt or http://secure.globalsign.com/cacert/stmtpmeccroot01.crt
STSAFE ECC Root CA 02	http://sw-center.st.com/STSAFE/STSAFEEccRootCA02.crt or https://sw-center.st.com/STSAFE/STSAFEEccRootCA02.crt
STM TPM ECC Intermediate CA 01	https://secure.globalsign.com/cacert/stmtpmeccint01.crt or http://secure.globalsign.com/stmtpmeccint01.crt
STM TPM ECC Intermediate CA 02	https://secure.globalsign.com/cacert/stmtpmeccint02.crt or http://secure.globalsign.com/stmtpmeccint02.crt
STM TPM ECC Intermediate CA 03	https://secure.globalsign.com/cacert/stmtpmeccint03.crt or http://secure.globalsign.com/stmtpmeccint03.crt
STM TPM ECC 384 Intermediate CA 01	https://secure.globalsign.com/cacert/stmtpmecc384int01.crt or http://secure.globalsign.com/stmtpmecc384int01.crt
STM TPM ECC 384 Intermediate CA 02	https://secure.globalsign.com/cacert/stmtpmecc384int02.crt or http://secure.globalsign.com/stmtpmecc384int02.crt
STMTPM ECC384 Intermediate CA 03 for CISCO	http://secure.globalsign.com/stmtpmecc384int03.crt or https://secure.globalsign.com/stmtpmecc384int03.crt
STSAFE TPM ECC Intermediate CA 10	http://sw-center.st.com/STSAFE/stsafetpmeccint10.crt or https://sw-center.st.com/STSAFE/stsafetpmeccint10.crt
STSAFE TPM ECC Intermediate CA 11	http://sw-center.st.com/STSAFE/stsafetpmeccint11.crt or https://sw-center.st.com/STSAFE/stsafetpmeccint11.crt
STSAFE TPM ECC Intermediate CA 20	http://sw-center.st.com/STSAFE/stsafetpmeccint20.crt or https://sw-center.st.com/STSAFE/stsafetpmeccint20.crt

Certificate common name	File/Link
STSAFE TPM ECC Intermediate CA 21	http://sw-center.st.com/STSAFE/stsafetpmeccint21.crt or https://sw-center.st.com/STSAFE/stsafetpmeccint21.crt

The STMicroelectronics CA infrastructure has been successfully audited by GlobalSign. The details of the infrastructure are available in the certificate practice statement (CPS) and certificate policy (CP) available at https://www.globalsign.com/en/repository/.

Revision history

Table 8. **Document revision history**

Date	Revision	Changes
02-Jun-2020	1	Initial release.
24-Jan-2023	2	Updated: • Table 1. List of products to add ST33TPHF2XSPI-C1, ST33KTPM2XSPI, ST33KTPM2XI2C, and ST33TPHF2XI2C-C1 • Section 1: TPM EK certificate content • Table 2. RSA intermediate CAs (for RSA 2048-bit EKs) and TPM products (at the time of publication) to update *ST Intermediate CA 06* row, and add *STSAFE TPM RSA Intermediate CA 10* row • Table 4. ECC intermediate CAs (for ECC_256 EKs) and TPM products (at the time of publication): updated title, updated *STM TPM ECC Intermediate CA 02* row, and added *STSAFE TPM ECC Intermediate CA 10* row • Table 5. ECC intermediate CAs (for ECC 384 EKs) and TPM products: updated title, updated *STM TPM ECC384 Intermediate CA 01* row, and added *STSAFE TPM ECC Intermediate CA 11* and *STM TPM ECC384 Intermediate CA 03 for CISCO* rows • Table 6. RSA TPM CA certificate URLs: added *STM TPM RSA root CA 02* and *STSAFE TPM RSA Intermediate CA 10* rows • Table 7. ECC TPM CA certificate URLs: added *STM TPM ECC Root CA 02*, *STMTPM ECC384 Intermediate CA 03 for Cisco*, *STSAFE TPM ECC Intermediate CA 10*, and *STSAFE TPM ECC Intermediate CA 11 rows*
22-Feb-2024	3	Updated Section Introduction. In Section 1: TPM EK certificate: • Added ST33KTPM2X, ST33KTPM2XSPI, STSAFE-TPM-V100 and ST33KTPM2I. • Added rows *STSAFE TPM RSA Intermediate CA 11*, *STSAFE TPM RSA Intermediate CA 20*, *STSAFE TPM ECC Intermediate CA 20* and *STSAFE TPM ECC Intermediate CA 21*. • Added Table 2. RSA intermediate CAs (for RSA 2048-bit EKs) and TPM products (at the time of publication)
08-Apr-2025	4	Updated . • Table 2. RSA intermediate CAs (for RSA 2048-bit EKs) and TPM products (at the time of publication) to update *STSAFE TPM RSA Intermediate CA 10* and *STSAFE TPM RSA Intermediate CA 20* rows • Table 3. RSA Intermediate CAs (for RSA 3072-bit EKs) and TPM products (at the time of publication): to update *STSAFE TPM RSA Intermediate CA 11* row, and add *STSAFE TPM RSA Intermediate CA 21* row • Table 4. ECC intermediate CAs (for ECC_256 EKs) and TPM products (at the time of publication): to update *STSAFE TPM ECC Intermediate CA 10* and *STSAFE TPM ECC Intermediate CA 20* rows • Table 5. ECC intermediate CAs (for ECC 384 EKs) and TPM products: to update *STSAFE TPM ECC Intermediate CA 11* and *STSAFE TPM ECC Intermediate CA 21* rows • Table 6. RSA TPM CA certificate URLs: added *STSAFE TPM RSA Intermediate CA 21* row

Contents

List of tables