

## 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          |                  |

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 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                  |                   |
| 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             |

| CA common name                    | Products         | Commercial part number | Firmware revision |
|-----------------------------------|------------------|------------------------|-------------------|
|                                   | 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             |

**Table 3. 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 | ST33HTPHAAH5            | 71.04             |
|                                | ST33TPHF2ESPI | ST33HTPHAAH6            | 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             |

| CA common name                    | Products      | Commercial part numbers | Firmware revision |
|-----------------------------------|---------------|-------------------------|-------------------|
|                                   | 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             |

**Table 4. ECC intermediate CAs (for ECC 384 EKs) and TPM products (at the time of publication)**

| 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             |

**Table 5. RSA TPM CA certificate URLs**

| Certificate common name         | File/Link  |
|---------------------------------|--|
| GlobalSign Trusted Computing CA | <a href="https://secure.globalsign.com/cacert/gstpmroot.crt">https://secure.globalsign.com/cacert/gstpmroot.crt</a> or <a href="http://secure.globalsign.com/cacert/gstpmroot.crt">http://secure.globalsign.com/cacert/gstpmroot.crt</a>                 |
| ST TPM Root certificate         | <a href="https://secure.globalsign.com/cacert/stmtpmekroot.crt">https://secure.globalsign.com/cacert/stmtpmekroot.crt</a> or <a href="http://secure.globalsign.com/cacert/stmtpmekroot.crt">http://secure.globalsign.com/cacert/stmtpmekroot.crt</a>     |
| STSAFE RSA Root CA 02           | <a href="http://sw-center.st.com/STSAFE/STSAFERsaRootCA02.crt">http://sw-center.st.com/STSAFE/STSAFERsaRootCA02.crt</a> or <a href="https://sw-center.st.com/STSAFE/STSAFERsaRootCA02.crt">https://sw-center.st.com/STSAFE/STSAFERsaRootCA02.crt</a>     |
| ST Intermediate CA 01           | <a href="https://secure.globalsign.com/cacert/stmtpmekint01.crt">https://secure.globalsign.com/cacert/stmtpmekint01.crt</a> or <a href="http://secure.globalsign.com/cacert/stmtpmekint01.crt">http://secure.globalsign.com/cacert/stmtpmekint01.crt</a> |
| ST Intermediate CA 02           | <a href="https://secure.globalsign.com/cacert/stmtpmekint02.crt">https://secure.globalsign.com/cacert/stmtpmekint02.crt</a> or <a href="http://secure.globalsign.com/cacert/stmtpmekint02.crt">http://secure.globalsign.com/cacert/stmtpmekint02.crt</a> |
| ST Intermediate CA 03           | <a href="https://secure.globalsign.com/cacert/stmtpmekint03.crt">https://secure.globalsign.com/cacert/stmtpmekint03.crt</a> or <a href="http://secure.globalsign.com/cacert/stmtpmekint03.crt">http://secure.globalsign.com/cacert/stmtpmekint03.crt</a> |
| ST Intermediate CA 04           | <a href="https://secure.globalsign.com/cacert/stmtpmekint04.crt">https://secure.globalsign.com/cacert/stmtpmekint04.crt</a> or <a href="http://secure.globalsign.com/cacert/stmtpmekint04.crt">http://secure.globalsign.com/cacert/stmtpmekint04.crt</a> |
| ST Intermediate CA 05           | <a href="https://secure.globalsign.com/cacert/stmtpmekint05.crt">https://secure.globalsign.com/cacert/stmtpmekint05.crt</a> or <a href="http://secure.globalsign.com/stmtpmekint05.crt">http://secure.globalsign.com/stmtpmekint05.crt</a>               |
| ST Intermediate CA 06           | <a href="https://secure.globalsign.com/cacert/stmtpmekint06.crt">https://secure.globalsign.com/cacert/stmtpmekint06.crt</a> or <a href="http://secure.globalsign.com/stmtpmekint06.crt">http://secure.globalsign.com/stmtpmekint06.crt</a>               |

| Certificate common name           | File/Link  |
|-----------------------------------|--|
| ST Intermediate CA 07             | <a href="https://secure.globalsign.com/cacert/stmtpmekint07.crt">https://secure.globalsign.com/cacert/stmtpmekint07.crt</a> or <a href="http://secure.globalsign.com/stmtpmekint07.crt">http://secure.globalsign.com/stmtpmekint07.crt</a>           |
| STSAFE TPM RSA Intermediate CA 10 | <a href="http://sw-center.st.com/STSAFE/stsafetpmrsaint10.crt">http://sw-center.st.com/STSAFE/stsafetpmrsaint10.crt</a> or <a href="https://sw-center.st.com/STSAFE/stsafetpmrsaint10.crt">https://sw-center.st.com/STSAFE/stsafetpmrsaint10.crt</a> |

**Table 6. ECC TPM CA certificate URLs**

| Certificate common name                        | File/Link  |
|--|--|
| GlobalSign Trusted Platform Module ECC Root CA | <a href="https://secure.globalsign.com/cacert/tpmeccroot.crt">https://secure.globalsign.com/cacert/tpmeccroot.crt</a> or <a href="http://secure.globalsign.com/cacert/tpmeccroot.crt">http://secure.globalsign.com/cacert/tpmeccroot.crt</a>                     |
| STM TPM ECC Root CA 01                         | <a href="https://secure.globalsign.com/cacert/stmtpmeccroot01.crt">https://secure.globalsign.com/cacert/stmtpmeccroot01.crt</a> or <a href="http://secure.globalsign.com/cacert/stmtpmeccroot01.crt">http://secure.globalsign.com/cacert/stmtpmeccroot01.crt</a> |
| STSAFE ECC Root CA 02                          | <a href="http://sw-center.st.com/STSAFE/STSAFEeccRootCA02.crt">http://sw-center.st.com/STSAFE/STSAFEeccRootCA02.crt</a> or <a href="https://sw-center.st.com/STSAFE/STSAFEeccRootCA02.crt">https://sw-center.st.com/STSAFE/STSAFEeccRootCA02.crt</a>             |
| STM TPM ECC Intermediate CA 01                 | <a href="https://secure.globalsign.com/cacert/stmtpmeccint01.crt">https://secure.globalsign.com/cacert/stmtpmeccint01.crt</a> or <a href="http://secure.globalsign.com/stmtpmeccint01.crt">http://secure.globalsign.com/stmtpmeccint01.crt</a>                   |
| STM TPM ECC Intermediate CA 02                 | <a href="https://secure.globalsign.com/cacert/stmtpmeccint02.crt">https://secure.globalsign.com/cacert/stmtpmeccint02.crt</a> or <a href="http://secure.globalsign.com/stmtpmeccint02.crt">http://secure.globalsign.com/stmtpmeccint02.crt</a>                   |
| STM TPM ECC Intermediate CA 03                 | <a href="https://secure.globalsign.com/cacert/stmtpmeccint03.crt">https://secure.globalsign.com/cacert/stmtpmeccint03.crt</a> or <a href="http://secure.globalsign.com/stmtpmeccint03.crt">http://secure.globalsign.com/stmtpmeccint03.crt</a>                   |
| STM TPM ECC 384 Intermediate CA 01             | <a href="https://secure.globalsign.com/cacert/stmtpmecc384int01.crt">https://secure.globalsign.com/cacert/stmtpmecc384int01.crt</a> or <a href="http://secure.globalsign.com/stmtpmecc384int01.crt">http://secure.globalsign.com/stmtpmecc384int01.crt</a>       |
| STM TPM ECC 384 Intermediate CA 02             | <a href="https://secure.globalsign.com/cacert/stmtpmecc384int02.crt">https://secure.globalsign.com/cacert/stmtpmecc384int02.crt</a> or <a href="http://secure.globalsign.com/stmtpmecc384int02.crt">http://secure.globalsign.com/stmtpmecc384int02.crt</a>       |
| STMTPM ECC384 Intermediate CA 03 for CISCO     | <a href="http://secure.globalsign.com/stmtpmecc384int03.crt">http://secure.globalsign.com/stmtpmecc384int03.crt</a> or <a href="https://secure.globalsign.com/stmtpmecc384int03.crt">https://secure.globalsign.com/stmtpmecc384int03.crt</a>                     |
| STSAFE TPM ECC Intermediate CA 10              | <a href="http://sw-center.st.com/STSAFE/stsafetpmeccint10.crt">http://sw-center.st.com/STSAFE/stsafetpmeccint10.crt</a> or <a href="https://sw-center.st.com/STSAFE/stsafetpmeccint10.crt">https://sw-center.st.com/STSAFE/stsafetpmeccint10.crt</a>             |
| STSAFE TPM ECC Intermediate CA 11              | <a href="http://sw-center.st.com/STSAFE/stsafetpmeccint11.crt">http://sw-center.st.com/STSAFE/stsafetpmeccint11.crt</a> or <a href="https://sw-center.st.com/STSAFE/stsafetpmeccint11.crt">https://sw-center.st.com/STSAFE/stsafetpmeccint11.crt</a>             |

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 7. Document revision history

| Date        | Revision    | Changes   |
|-------------|-------------|---|
| 02-Jun-2020 | 1           | Initial release.  |
| 2           | 24-Jan-2023 | Updated: <ul style="list-style-type: none"> <li>• <a href="#">Table 1. List of products</a> to add ST33TPHF2XSPI-C1, ST33KTPM2XSPI, ST33KTPM2XI2C, and ST33TPHF2XI2C-C1</li> <li>• <a href="#">Section 1 TPM EK certificate content</a></li> <li>• <a href="#">Table 2. RSA intermediate CAs and TPM products (at the time of publication)</a> to update <i>ST Intermediate CA 06</i> row, and add <i>STSAFE TPM RSA Intermediate CA 10</i> row</li> <li>• <a href="#">Table 3. ECC intermediate CAs (for ECC_256 EKs) and TPM products (at the time of publication)</a>: updated title, updated <i>STM TPM ECC Intermediate CA 02</i> row, and added <i>STSAFE TPM ECC Intermediate CA 10</i> row</li> <li>• <a href="#">Table 4. ECC intermediate CAs (for ECC 384 EKs) and TPM products (at the time of publication)</a>: updated title, updated <i>STM TPM ECC384 Intermediate CA 01</i> row, and added <i>STSAFE TPM ECC Intermediate CA 11</i> and <i>STM TPM ECC384 Intermediate CA 03 for CISCO</i> rows</li> <li>• <a href="#">Table 5. RSA TPM CA certificate URLs</a>: added <i>STM TPM RSA root CA 02</i> and <i>STSAFE TPM RSA Intermediate CA 10</i> rows</li> <li>• <a href="#">Table 6. ECC TPM CA certificate URLs</a>: added <i>STM TPM ECC Root CA 02</i>, <i>STMTPM ECC384 Intermediate CA 03 for Cisco</i>, <i>STSAFE TPM ECC Intermediate CA 10</i>, and <i>STSAFE TPM ECC Intermediate CA 11</i> rows</li> </ul> |

## Contents

|          |                                 |          |
|----------|---------------------------------|----------|
| <b>1</b> | <b>TPM EK certificate .....</b> | <b>2</b> |
|          | <b>Revision history .....</b>   | <b>6</b> |
|          | <b>List of tables .....</b>     | <b>8</b> |

## List of tables

|                 |  |   |
|-----------------|--|---|
| <b>Table 1.</b> | List of products . . . . .   | 1 |
| <b>Table 2.</b> | RSA intermediate CAs and TPM products (at the time of publication) . . . . .                   | 2 |
| <b>Table 3.</b> | ECC intermediate CAs (for ECC_256 EKs) and TPM products (at the time of publication) . . . . . | 3 |
| <b>Table 4.</b> | ECC intermediate CAs (for ECC 384 EKs) and TPM products (at the time of publication) . . . . . | 4 |
| <b>Table 5.</b> | RSA TPM CA certificate URLs . . . . .  | 4 |
| <b>Table 6.</b> | ECC TPM CA certificate URLs . . . . .  | 5 |
| <b>Table 7.</b> | Document revision history . . . . .  | 6 |



**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. 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.

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 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.

ST and the ST logo are trademarks of ST. For additional information about ST trademarks, refer to [www.st.com/trademarks](http://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.

© 2023 STMicroelectronics – All rights reserved