

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

Data brief



### Description

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

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

Downloadable links to ST TPM EK certificate files are provided.

### Features

- ST TPM endorsement key (EK) certificates
- Provided in X.509 format
- Root signed by independent CA (Globalsign®)
- Using dedicated intermediate certificates to differentiate various ST TPM product technologies or final applications

# 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 certification authority (CA) GlobalSign.

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 1. RSA intermediate CAs and TPM products (at the time of publication)**

| CA common name        | Product line  | Commercial part number | Firmware revision |
|-----------------------|---------------|------------------------|-------------------|
| ST Intermediate CA 01 | ST19TPM12LPC  | ST19NP18PVMT           | 08.08             |
|                       | ST19TPM12LPC  | ST19NP18PVMK           | 08.28             |
|                       | ST19TPM12LPC  | ST19NP18PVMO           | 08.32             |
| 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             |
| ST33TPHF2ESPI         | ST33HTPHAHC8  | 73.16                  |                   |
| ST33TPHF20SPI         | ST33HTPHAHC9  | 74.16                  |                   |
| ST Intermediate CA 06 | ST33TPHF2XSPI | ST33HTPHAHC4           | 01.256            |
|                       | ST33TPHF2XI2C | ST33HTPHAHC5           | 02.256            |
| ST Intermediate CA 07 | ST33GTPMASPI  | ST33GTPMA020FAE5       | 03.256            |
|                       | ST33GTPMAI2C  | ST33GTPMA020FAE6       | 06.256            |

**Table 2. ECC intermediate CAs (ECC\_256) and TPM products (at the time of publication)**

| CA common name                    | Product line  | Commercial part numbers | Firmware revision |
|-----------------------------------|---------------|-------------------------|-------------------|
| STM TPM ECC<br>Intermediate CA 01 | ST33TPHF2ESPI | ST33HTPHAAE5            | 71.00             |
|                                   | ST33TPHF2ESPI | ST33HTPHAAE6            | 71.00             |
|                                   | ST33TPHF20SPI | ST33HTPHAAE8            | 72.00             |
|                                   | ST33TPHF2ESPI | ST33HTPHAA5             | 71.04             |
|                                   | ST33TPHF2ESPI | ST33HTPHAA6             | 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             |
|                                   | ST33TPHF2ESPI | ST33HTPHAHC8            | 73.16             |
| ST33TPHF20SPI                     | ST33HTPHAHC9  | 74.16                   |                   |
| STM TPM ECC<br>Intermediate CA 02 | ST33TPHF2XSPI | ST33HTPHAHC4            | 01.256            |
|                                   | ST33TPHF2XI2C | ST33HTPHAHC5            | 02.256            |
| STM TPM ECC<br>Intermediate CA 03 | ST33GTPMASPI  | ST33GTPMA020FAE5        | 03.256            |
|                                   | ST33GTPMAI2C  | ST33GTPMA020FAE6        | 06.256            |

**Table 3. ECC intermediate CAs (ECC 384) and TPM products (at the time of publication)**

| CA common name                       | Product line  | Commercial part numbers | Firmware revision |
|--------------------------------------|---------------|-------------------------|-------------------|
| STM TPM ECC384<br>Intermediate CA 01 | ST33TPHF2XSPI | ST33HTPHAHC4            | 01.256            |
|                                      | ST33TPHF2XI2C | ST33HTPHAHC5            | 02.256            |
| STM TPM ECC384<br>Intermediate CA 02 | ST33GTPMASPI  | ST33GTPMA020FAE5        | 03.256            |
|                                      | ST33GTPMAI2C  | ST33GTPMA020FAE6        | 06.256            |

**Table 4. 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<br><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<br><a href="http://secure.globalsign.com/cacert/stmtpmekroot.crt">http://secure.globalsign.com/cacert/stmtpmekroot.crt</a>     |
| ST Intermediate CA 01           | <a href="https://secure.globalsign.com/cacert/stmtpmekint01.crt">https://secure.globalsign.com/cacert/stmtpmekint01.crt</a> or<br><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<br><a href="http://secure.globalsign.com/cacert/stmtpmekint02.crt">http://secure.globalsign.com/cacert/stmtpmekint02.crt</a> |

**Table 4. RSA TPM CA certificate URLs (continued)**

| Certificate common name | File/Link  |
|-------------------------|--|
| 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>               |
| 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>               |

**Table 5. 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> |
| 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>       |

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/>.

## 2 Revision history

**Table 6. Document revision history**

| Date        | Revision | Changes  |
|-------------|----------|--|
| 27-Jul-2015 | 1        | Initial release.   |
| 18-Mar-2016 | 2        | Updated <i>Table 1: RSA intermediate CAs and TPM products (as of the document revision date)</i> .<br>Added <i>Table 2: ECC Intermediate CAs and TPM products (as of the document revision date)</i> .<br>Updated <i>Table 3: TPM CA certificate URLs</i> .<br>Added <i>Table 4: ECC TPM CA certificate URLs</i> . |
| 05-Sep-2016 | 3        | Updated <i>Table 1: RSA intermediate CAs and TPM products (as of the document revision date)</i> .<br>Updated <i>Table 2: ECC Intermediate CAs and TPM products (as of the document revision date)</i> .   |
| 22-May-2019 | 4        | Document reference updated.<br>Updated all tables and added new ones.  |

**IMPORTANT NOTICE – PLEASE 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 acknowledgement.

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, please 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.

© 2019 STMicroelectronics – All rights reserved