STSW-TPMCERT1

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 ST19TPM12LPC ST19TPM12LPC	ST19NP18PVMT ST19NP18PVMK ST19NP18PVMO	08.08 08.28 08.32
ST Intermediate CA 02	ST33TPM12LPC ST33TPM12LPC ST33TPM12I2C ST33TPM12SPI ST33TPM12LPC	ST33ZP24PVSC ST33ZP24PVSH ST33ZP24PVSK ST33ZP24PVSL ST33ZP24PVSP	13.00 13.08 13.10 13.11 13.12
ST Intermediate CA 03	ST33TPM12LPC	ST33ZP24PVSM	13.08
ST Intermediate CA 04	ST33TPMF2ESPI ST33TPMF2ESPI	ST33HTPMAAD8 ST33HTPMAAE0	70.00 70.00
ST Intermediate CA 05	ST33TPHF2ESPI ST33TPHF2ESPI ST33TPHF20SPI ST33TPHF2ESPI ST33TPHF2ESPI ST33TPHF2ESPI ST33TPHF2ESPI ST33TPHF20SPI ST33TPHF2ESPI ST33TPHF2ESPI ST33TPHF2EI2C ST33TPHF2EI2C ST33TPHF20I2C ST33TPHF2ESPI ST33TPHF20SPI ST33TPHF2EI2C ST33TPHF20I2C ST33TPHF2ESPI ST33TPHF20SPI	ST33HTPHAAE5 ST33HTPHAAE6 ST33HTPHAAE8 ST33HTPHAHA5 ST33HTPHAHA6 ST33HTPHAAF0 ST33HTPHAAF1 ST33HTPHAAF3 ST33HTPHAHB3 ST33HTPHAHB4 ST33HTPHAHB7 ST33HTPHAHB8 ST33HTPHAHB9 ST33HTPHAHC0 ST33HTPHAHC1 ST33HTPHAHC2 ST33HTPHAHC3 ST33HTPHAHC8 ST33HTPHAHC9	71.00 71.00 72.00 71.04 71.04 73.00 73.00 74.00 73.04 73.04 73.05 73.05 74.05 73.08 74.08 73.09 74.09 73.16 74.16
ST Intermediate CA 06	ST33TPHF2XSPI ST33TPHF2XI2C	ST33HTPHAHC4 ST33HTPHAHC5	01.256 02.256
ST Intermediate CA 07	ST33GTPMASPI ST33GTPMAI2C	ST33GTPMA020FAE5 ST33GTPMA020FAE6	03.256 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 Intermediate CA 01	ST33TPHF2ESPI ST33TPHF2ESPI ST33TPHF20SPI ST33TPHF2ESPI ST33TPHF2ESPI ST33TPHF2ESPI ST33TPHF2ESPI ST33TPHF2ESPI ST33TPHF20SPI ST33TPHF2EI2C ST33TPHF2EI2C ST33TPHF20I2C ST33TPHF2ESPI ST33TPHF20SPI ST33TPHF2EI2C ST33TPHF20I2C ST33TPHF2ESPI ST33TPHF20SPI	ST33HTPHAAE5 ST33HTPHAAE6 ST33HTPHAAE8 ST33HTPHAHA5 ST33HTPHAHA6 ST33HTPHAAF0 ST33HTPHAAF1 ST33HTPHAHB3 ST33HTPHAHB4 ST33HTPHAAF3 ST33HTPHAHB7 ST33HTPHAHB8 ST33HTPHAHB9 ST33HTPHAHC0 ST33HTPHAHC1 ST33HTPHAHC2 ST33HTPHAHC3 ST33HTPHAHC8 ST33HTPHAHC9	71.00 71.00 72.00 71.04 71.04 73.00 73.00 73.04 73.04 74.00 73.05 73.05 74.05 73.08 74.08 73.09 74.09 73.16 74.16
STM TPM ECC Intermediate CA 02	ST33TPHF2XSPI ST33TPHF2XI2C	ST33HTPHAHC4 ST33HTPHAHC5	01.256 02.256
STM TPM ECC Intermediate CA 03	ST33GTPMASPI ST33GTPMAI2C	ST33GTPMA020FAE5 ST33GTPMA020FAE6	03.256 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 Intermediate CA 01	ST33TPHF2XSPI ST33TPHF2XI2C	ST33HTPHAHC4 ST33HTPHAHC5	01.256 02.256
STM TPM ECC384 Intermediate CA 02	ST33GTPMASPI ST33GTPMAI2C	ST33GTPMA020FAE5 ST33GTPMA020FAE6	03.256 06.256

Table 4. 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
ST Intermediate CA 01	https://secure.globalsign.com/cacert/stmtpmekint01.crt or http://secure.globalsign.com/cacert/stmtpmekint01.crt
ST Intermediate CA 02	https://secure.globalsign.com/cacert/stmtpmekint02.crt or http://secure.globalsign.com/cacert/stmtpmekint02.crt

Table 4. RSA TPM CA certificate URLs (continued)

Certificate common name	File/Link
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

Table 5. 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
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

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 *Table 1: RSA intermediate CAs and TPM products (as of the document revision date)*. Added *Table 2: ECC Intermediate CAs and TPM products (as of the document revision date)*. Updated *Table 3: TPM CA certificate URLs*. Added *Table 4: ECC TPM CA certificate URLs*.
05-Sep-2016	3	Updated *Table 1: RSA intermediate CAs and TPM products (as of the document revision date)*. Updated *Table 2: ECC Intermediate CAs and TPM products (as of the document revision date)*.
22-May-2019	4	Document reference updated. Updated all tables and added new ones.